GUIA DE BOAS PRÁTICAS
LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)



Abril/2020

gov.br

Comitê Central de Governança de Dados

Advocacia Geral da União
Caio Castelliano de Vasconcelos (Tilular)
Eduardo Alexandre Lang (Suplente)

Casa Civil
Orlando Oliveira dos Santos (Titular)
Marcelo Amaro Buz (Suplente)

Controladoria Geral da União
Marcio Denyz Pessanha Gonçalves (Titular)
Karin Webster (Suplente)

Instituto Nacional de Seguro Social
Marcia Eliza de Souza (Titular)
Flávio Ferreira dos Santos (Suplente)

Secretaria Especial de Desburocratização, Gestão e Governo Digital
Ciro Pitangueira de Avelino (Titular)
Renan Mendes Gaya Lopes dos Santos (Suplente)

Secretaria Especial de Modernização do Estado
Nizar Ratib Midrei (Titular)
Sylvio Cezar Koury Musolino Filho (Suplente)

Receita Federal do Brasil
Moacyr Mondardo Junior (Titular)
Juliano Brito da Justa Neves (Suplente)

Equipe Técnica de Elaboração

Advocacia Geral da União
Victor Cravo (Titular)
Murillo Cesar de Mello Brandão Filho (Suplente)

Casa Civil
Nadia Lopes Cerqueira (Titular)
Mauricio Augusto Coelho (Suplente)

Controladoria Geral da União
Marcos Gerhardt Lindenmayer (Titular)
Marcio Denyz Pessanha Gonçalves (Suplente)
Genelice Paiva da Costa (Apoio Técnico)
Roberto Kodama (Apoio Técnico)

Gabinete de Segurança Institucional
Luiz Octavio de Souza Pereira Gomes (Titular)
Arthur Pereira Sabbat (Suplente)

Instituto Nacional de Seguro Social
Cibelle Cesar do Amaral Brasil (Titular)

Secretaria Especial de Desburocratização, Gestão e Governo Digital
Anderson Sousa de Araújo (Titular)
Loriza Andrade Vaz de Melo (Suplente)
Julierme Rodrigues da Silva (Apoio Técnico)
Luiz Henrique Espírito Santo (Apoio Técnico)

Secretaria Especial de Modernização do Estado
Sylvio Cezar Koury Musolino Filho (Titular)
Clarice G. Oliveira (Suplente)

Receita Federal do Brasil
Danielle Carvalho Barbosa (Titular)
Lucas Borges Monteiro (Suplente)

LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Guia de Boas Práticas para Implementação na Administração Pública Federal

HISTÓRICO DE VERSÕES

DATA	VERSÃO	DESCRIÇÃO	AUTOR
23/03/2020	1.0	Primeira versão do Guia de Boas Práticas.	Equipe Técnica de Elaboração

SUMÁRIO

INTRODUÇÃO

A governança no compartilhamento de dados na administração pública federal, autárquica e fundacional segue as diretrizes estabelecidas no Decreto nº 10.046, de 9 de outubro de 2019, e precisa ser compreendida à luz das restrições legais, dos requisitos de segurança da informação e comunicações e do disposto pela Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

Nesse contexto, este documento tem como objetivo fornecer orientações de boas práticas aos órgãos e entidades da Administração Pública Federal direta, autárquica e fundacional para as operações de tratamento de dados pessoais, conforme previsto no art. 50 da LGPD.

Inicialmente, a adequação dos órgãos e entidades em relação à LGPD envolve uma transformação cultural que deve alcançar os níveis estratégico, tático e operacional da instituição. Essa transformação envolve: considerar a privacidade dos dados pessoais do cidadão desde a fase de concepção do serviço ou produto até sua execução (Privacidade by Design); e promover ações de conscientização de todo corpo funcional no sentido de incorporar o respeito à privacidade dos dados pessoais nas atividades institucionais cotidianas.

Cumpre destacar que o princípio da finalidade do tratamento de dados estabelecido na LGPD exige que os propósitos do tratamento sejam legítimos, específicos, explícitos e informados ao titular. O tratamento posterior somente será possível se for compatível com esses propósitos e finalidades (art. 6º, I). No caso do setor público, a finalidade relaciona-se com a execução de políticas públicas, devidamente estabelecida em lei, e com o cumprimento de obrigação legal ou regulatória pelo controlador. O consentimento, quando exigido pelos órgãos públicos, será medida excepcional e deverá se referir a finalidades determinadas e comunicadas claramente ao titular do dado.

As orientações relativas ao tratamento dos dados pessoais pela Administração Pública Federal (APF) constante deste documento foram estruturadas em quatro capítulos:

- O Capítulo 1 contempla a base legal de tratamento, exercícios do direito do titular de dados e base legal de tratamento;
- O Capítulo 2 indica como realizar o tratamento de dados pessoais e elaborar o Relatório de Impacto de Proteção à Privacidade de Dados Pessoais;
- O Capítulo 3 descreve o ciclo de vida de tratamento dos dados pessoais; e
- O Capítulo 4 apresenta padrões e frameworks de segurança da informação.

Este documento, que será atualizado, aperfeiçoado, ampliado permanentemente, tem por objeto o contato inicial e a familiarização com o novo universo da proteção e tratamento de dados pessoais. Neste momento, não há aqui o propósito de se apresentar uma metodologia de implementação da LGPD ou abranger e esgotar todos os aspectos de tal Lei, uma vez que algumas diretrizes de proteção de dados da LGPD necessitam de detalhamento, em regulamentos e procedimentos próprios, a serem editados pela Autoridade Nacional de Proteção de Dados.

1 DIREITOS FUNDAMENTAIS DO TITULAR DOS DADOS

1.1 BASE LEGAL PARA TRATAMENTO DOS DADOS PESSOAIS

A **Lei Geral de Proteção de Dados Pessoais** (LGPD – Lei nº 13.709/2018) foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. Essa Lei versa sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.

No âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por dois "agentes de tratamento", o Controlador e o Operador:

- O Controlador é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No âmbito da Administração Pública, o Controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade imbuída de adotar as decisões acerca do tratamento de tais dados.
- O Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas daquela representada pelo Controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere.

Considera-se "tratamento de dados" qualquer atividade que utilize um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Essas operações de tratamento são destacadas a seguir:

ACESSO - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;

ARMAZENAMENTO - ação ou resultado de manter ou conservar em repositório um dado;

ARQUIVAMENTO - ato ou efeito de manter registrado um dado embora já tenha perdido a validade ou esgotado a sua vigência;

AVALIAÇÃO - analisar o dado com o objetivo de produzir informação;

CLASSIFICAÇÃO - maneira de ordenar os dados conforme algum critério estabelecido;

COLETA - recolhimento de dados com finalidade específica;

COMUNICAÇÃO - transmitir informações pertinentes a políticas de ação sobre os dados;

CONTROLE - ação ou poder de regular, determinar ou monitorar as ações sobre o dado;

DIFUSÃO - ato ou efeito de divulgação, propagação, multiplicação dos dados;

DISTRIBUIÇÃO - ato ou efeito de dispor de dados de acordo com algum critério estabelecido;

ELIMINAÇÃO - ato ou efeito de excluir ou destruir dado do repositório;

EXTRAÇÃO - ato de copiar ou retirar dados do repositório em que se encontrava;

MODIFICAÇÃO - ato ou efeito de alteração do dado;

PROCESSAMENTO - ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;

PRODUÇÃO - criação de bens e de serviços a partir do tratamento de dados;

RECEPÇÃO - ato de receber os dados ao final da transmissão;

REPRODUÇÃO - cópia de dado preexistente obtido por meio de qualquer processo;

TRANSFERÊNCIA - mudança de dados de uma área de armazenamento para outra, ou para terceiro;

TRANSMISSÃO - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc.;

UTILIZAÇÃO - ato ou efeito do aproveitamento dos dados.

Ademais, é importante esclarecer que, por taxativa previsão da LGPD (Art. 4˚), as disposições da Lei não são aplicadas ao tratamento de dados pessoais nas seguintes situações:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente jornalísticos, artístico e acadêmico (aplicando-se a esta última hipótese os arts. 7º e 11 da LGPD);

III - realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, ou;

IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

Os casos de tratamento de dados que estão previstos e permitidos pela LGPD serão explicados a seguir. Mas é muito importante destacar que eles não são amplos e absolutos; ao contrário, existem limites para essa operação que estão dados pela boa-fé e demais princípios previstos no Art. 6º da mesma norma.

Antes de iniciar alguma espécie de tratamento de dados pessoais, o agente deve se certificar previamente que a finalidade da operação esteja registrada de forma clara e explícita e os propósitos especificados e informados ao titular dos dados.

No caso do setor público, a principal finalidade do tratamento está relacionada à execução de políticas públicas, devidamente previstas em lei, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. O tratamento para cumprimento de obrigação legal ou regulatória pelo controlador também é uma hipótese corriqueira no serviço público. Nessas duas situações, o consentimento do titular de dados é dispensado.

Por outro lado, em hipóteses bastante específicas, o consentimento do titular pode ser necessário para finalidades determinadas. Quando isso ocorrer, as autorizações genéricas para o tratamento de dados pessoais serão consideradas nulas.

Além disso, no tratamento feito pelo poder público, as regras previstas nos artigos 23 (procedimentos de atuação) e 30 (regulamentos da ANPD) da LGPD sempre devem ser seguidas de forma complementar.

A LGPD previu expressamente em seu artigo 7˚, dez hipóteses de tratamento de dados, bem como estabeleceu os requisitos para execução de tal procedimento. São as chamadas bases legais de tratamento de dados pessoais.

Entre essas hipóteses, vamos ressaltar neste documento o tratamento de dados pessoais pela Administração Pública Federal, citada no inciso III.

Nesses casos, é possível o compartilhamento de dados com órgãos públicos ou transferência de dados a terceiro fora do setor público. Quando isso acontecer, os agentes de tratamento devem comunicar as operações executadas, de forma clara, aos titulares dos dados. É importante registrar que tal comunicação deve ser renovada na alteração da finalidade ou em qualquer alteração nas

operações de tratamento, inclusive de novo compartilhamento ou transferência.

O compartilhamento dentro da administração pública no âmbito da execução de políticas públicas é previsto na lei e dispensa o consentimento específico. Contudo, o órgão que coleta deve informar claramente que o dado será compartilhado e com quem. Do outro lado, o órgão que solicita acesso a dado colhido por outro, isto é, solicita receber o compartilhamento, precisa justificar esse acesso com base na execução de uma política pública específica e claramente determinada, descrevendo o motivo da solicitação de acesso e o uso que será feito com os dados. Informações protegidas por sigilo seguem protegidas e sujeitas a normativos e regras específicas. Na sequência, são apresentadas considerações sobre as hipóteses legais de tratamento de dados da LGPD. A seção 2.1 abordará questões fundamentais a serem observadas pelos órgãos e entidades da administração federal no sentido de assegurar a conformidade do tratamento de dados pessoais de acordo com as referidas hipóteses legais e princípios da LGPD.

I - mediante o fornecimento de consentimento pelo titular

Hipótese que exige consentimento do titular do dado. Trata-se da regra da autonomia da vontade. É a manifestação livre e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

O titular dos dados tem liberdade para autorizar, negar ou revogar (reconsiderar) autorização anteriormente concedida para tratamento de seus dados pessoais.

Trata-se de consentimento altamente qualificado, já que a manifestação de vontade precisa ser (I) livre e inequívoca; (II) formada mediante o conhecimento de todas as informações necessárias para tal, o que inclui a finalidade do tratamento de dados e eventual compartilhamento; e (III) restrita às finalidades específicas e determinadas que foram informadas ao titular dos dados.

O ônus da prova do consentimento cabe ao controlador, sendo proibido o tratamento de dados pessoais mediante vício de consentimento.

O consentimento também pode ser tácito quando o titular do dado o torna manifestamente público previamente. Tal situação está prevista no §4° do Art. 7°: "É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei."

O controlador que obtiver o consentimento e necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas em Lei.

II - para o cumprimento de obrigação legal ou regulatória pelo controlador

Hipótese que dispensa o consentimento do titular do dado. É a regra da legalidade ampla e da preservação do interesse público sobre o particular. Esse é um autorizador da LGPD que possibilita que a lei não entre em conflito com outras legislações ou regulamentos vigentes. No Anexo II deste documento, constam previsões normativas que autorizam tratamento de dados extra LGPD; entre elas, a Lei de Acesso à Informação (Lei nº 12.527/2011 - LAI), a do processo administrativo na administração pública federal (Lei nº 9.784/1999) e o Marco Civil da Internet (Lei nº 12.965/2014).

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV da Lei

Hipótese que dispensa o consentimento do titular do dado. É o tratamento de dados feito com a finalidade específica da execução de política pública formalmente instituída por Lei ou Ato administrativo. O instrumento que fixa a política pública que autoriza o tratamento do dado pessoal pode ser desde uma norma formal até um contrato ou instrumento congênere. É importante ressaltar que este tipo de tratamento independe de consentimento do titular e deve respeitar as regras previstas pelos artigos 23 a 30 da LGPD.

Sempre que a administração pública efetuar o tratamento de dados pessoais no exercício de suas competências legais vinculadas a políticas públicas e entrega de serviços públicos, não precisará colher o consentimento; mas, necessariamente, será obrigada a informar a finalidade e a

forma como o dado será tratado.

Todas as regras descritas pelos Artigos 23 a 30 da LGPD devem ser observadas pelos órgãos e entidades públicas. As ações destacadas a seguir são de especial importância para viabilizar o tratamento dos dados pelo poder público:

- informar as hipóteses em que, no exercício de suas competências, o órgão respalda o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos (Art. 23, I);

- indicar encarregado quando realizar operações de tratamento de dados pessoais, nos termos do art. 39 da LGPD (Art. 23, II);

- observar as formas de publicidade das operações de tratamento que poderão ser estabelecidas pela Autoridade Nacional de Proteção de Dados (ANPD, Art. 23, § 1º);

- manter os dados em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral. (Art. 25); e

- realizar o uso compartilhado de dados pessoais de acordo com as finalidades específicas de execução de políticas públicas e atribuição legal do órgão ou entidade, respeitados os princípios de proteção de dados pessoais elencados no art. 6º da LGPD (Art. 26).

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais

Hipótese que dispensa o consentimento do titular do dado. Utilização estrita para realização de estudos por órgão de pesquisa público ou privado.

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados

Hipótese de consentimento específico do titular para utilização na execução ou na preparação de negócio jurídico em que seja parte.

No caso de haver necessidade de processamento de dado pessoal para a consecução dos termos ajustados em contrato, o consentimento do titular estará abrangido pela autonomia da vontade expressa no momento da formalização do contrato, não sendo necessária nova previsão expressa para o tratamento decorrente do negócio. São exemplos de tratamento sem previsão expressa: enviar comunicado ou notificação; processar pagamentos.

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem)

Hipótese que dispensa o consentimento do titular do dado. Previsão para exercício regular de direito, incluindo contraditório, ampla defesa e devido processo legal. Trata-se de ressalva para esclarecer que a proteção aos dados pessoais não compromete o direito que as partes têm de produzir provas umas contra as outras, ainda que estas se refiram a dados pessoais do adversário; ou seja, que não cabe oposição ao tratamento de dados pessoais no contexto dos processos judiciais, administrativos e arbitrais.

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro

Hipótese que dispensa o consentimento do titular do dado nos casos de necessidade de tutela do bem maior da pessoa natural, a vida e sua incolumidade, ambos inseridos no conceito de dignidade da pessoa humana como fundamento da República.

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária

Hipótese que dispensa o consentimento do titular do dado nos casos de estrita necessidade

de tutela da saúde do titular, de terceiro ou pública. É a única hipótese de tratamento de dado manejado por agente exclusivo: profissionais de saúde, serviços de saúde ou autoridade sanitária.

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais

Hipótese que dispensa o consentimento do titular do dado. É uma previsão geral e subsidiária, mediante prévia e expressa motivação pelo controlador da finalidade e necessidade (legítimo interesse) do tratamento.

O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I – apoio e promoção de atividades do controlador; II – proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos da LGPD.

Em tais circunstâncias, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, devendo o controlador adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

Convém salientar que o tratamento autorizado por esta hipótese traz consigo conjunto adicional de medidas de salvaguarda dos dados, inclusive com a possibilidade de a ANPD solicitar ao controlador relatórios de impacto à proteção de dados pessoais, justamente pelo risco de violação que tal hipótese acarreta, em particular, para entidades privadas. A elaboração do referido relatório de impacto é abordada na seção 2.5 deste documento.

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente

Hipótese que dispensa o consentimento do titular do dado. Previsão para os casos estritos de tutela do crédito. Há expressa necessidade de observância simultânea da legislação pertinente.

1.2 DIREITOS DO TITULAR

A LGPD estabeleceu uma estrutura legal que empodera os titulares de dados pessoais, fornecendo-lhes direitos a serem exercidos perante os controladores de dados. Esses direitos devem ser garantidos durante toda a existência do tratamento dos dados pessoais do titular realizado pelo órgão ou entidade.

Os direitos a serem garantidos aos titulares de dados estão organizados nas tabelas a seguir, as quais estão segregadas em direitos decorrentes dos princípios estabelecidos pelo art. 6º da LGPD e em direitos específicos dos titulares constantes dos demais artigos da referida Lei.

Tabela 1 Direitos garantidos aos titulares de dados

DIREITOS DOS TITULARES DE DADOS QUE DECORREM DOS PRINCÍPIOS	PRINCÍPIO CORRESPONDENTE	REFERÊNCIA LEGISLATIVA (LGPD)
Direito ao tratamento adstrito aos propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades	Princípio da finalidade	Art. 6º, I

Direito ao tratamento adequado, compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento	Princípio da adequação	Art. 6º, II
Direito à limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento	Princípio da necessidade	Art. 6º, III
Direito à consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais	Princípio do livre acesso	Art. 6º, IV
Direito à exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento	Princípio da qualidade dos dados	Art. 6º, V
Direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial	Princípio da transparência	Art. 6º, VI
Direito à segurança dos dados, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão	Princípio da segurança	Art. 6º, VII
Direito à adequada prevenção de danos, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais	Princípio da prevenção	Art. 6º, VIII
Direito de não ser discriminado de forma ilícita ou abusiva	Princípio da não discriminação	Art. 6º, IX
Direito de exigir a adequada responsabilização e a prestação de contas por parte dos agentes de tratamento, ao qual se contrapõe o dever, por parte destes, de adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais	Princípio da responsabilização e prestação de contas	Art. 6º, X

Além dos direitos dos titulares de dados que são decorrentes do art. 6º da LGPD, a Lei apresenta diretos específicos dos titulares de dados, que são destacados na tabela abaixo.

Tabela 2 Diretos específicos dos titulares de dados

DIREITOS DOS TITULARES DE DADOS QUE DECORREM DOS PRINCÍPIOS	REFERÊNCIA LEGISLATIVA (LGPD)
Direito de condicionar o tratamento de dados ao prévio consentimento expresso, inequívoco e informado do titular, salvo as exceções legais	Arts. 7º, I, e 8º
Direito de exigir o cumprimento de todas as obrigações de tratamento previstas na lei, mesmo para os casos de dispensa de exigência de consentimento	Art. 7º, § 6º
Direito à inversão do ônus da prova quanto ao consentimento	Art. 8º, § 2º
Direito de requerer a nulidade de autorizações genéricas para o tratamento de dados pessoais	Art. 8º, § 4º
Direito de requerer a nulidade do consentimento caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou, ainda, não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca	Art. 9º, § 1º
Direito de requerer a revogação do consentimento a qualquer tempo, mediante manifestação expressa do titular, por procedimento gratuito e facilitado	Art. 8º, § 5º
Direito de revogar o consentimento caso o titular discorde das alterações quanto ao tratamento de dados, seja na finalidade, forma e duração do tratamento, alteração do controlador ou compartilhamento	Arts. 8º, § 6º e 9º, § 2º
Direito de acesso facilitado ao tratamento de dados, cujas informações devem ser disponibilizadas de forma clara, adequada e ostensiva acerca de (entre outras): finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador; finalidade, responsabilidades dos agentes que realizarão o tratamento e direitos do titular, com menção explícita aos direitos contidos no art. 18	Art. 9º
Direito de ser informado sobre aspectos essenciais do tratamento de dados, com destaque específico sobre o teor das alterações supervenientes no tratamento	Art. 8º, § 6º
Direito de ser informado, com destaque, sempre que o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço, ou, ainda, para o exercício de direito, o que se estende à informação sobre os meios pelos quais o titular poderá exercer seus direitos	Art. 9º, § 3º
Direito de ser informado sobre a utilização dos dados pela administração pública para os fins autorizados pela lei e para a realização de estudos por órgão de pesquisa	Art. 7º, III e IV c/c art. 7º, § 1º
Direito de que o tratamento de dados pessoais cujo acesso é público esteja adstrito à finalidade, à boa-fé e ao interesse público que justificaram sua disponibilização	Art. 7º, § 3º

Direito de condicionar o compartilhamento de dados por determinado controlador que já obteve consentimento a novo e específico consentimento. No caso da Administração Pública Federal (APF), em que o tratamento é embasado nas hipóteses de dispensa de consentimento original, o compartilhamento demandará uma nova justificativa de tratamento	Art. 7º, § 5º
Direito de ter o tratamento de dados limitado ao estritamente necessário para a finalidade pretendida quando o tratamento for baseado no legítimo interesse do controlador	Art. 10, § 1º
Direito à transparência do tratamento de dados baseado no legítimo interesse do controlador	Art. 10, § 2º
Direito à anonimização dos dados pessoais sensíveis, sempre que possível, na realização de estudos por órgão de pesquisa	Art. 11, II, c
Direito de ter a devida publicidade em relação às hipóteses de dispensa de consentimento para: tratamento de dados sensíveis no cumprimento de obrigação legal ou regulatória pelo controlador; ou tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos	Art. 11, § 2º
Direito de impedir a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde, com o objetivo de obter vantagem econômica (exceto nos casos de portabilidade de dados quando consentido pelo titular)	Art. 11, § 4º
Direito de que os dados pessoais sensíveis utilizados em estudos de saúde pública sejam tratados exclusivamente dentro do órgão de pesquisa e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas	Art. 13
Direito de não ter dados pessoais revelados na divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa sobre saúde pública	Art. 13, § 1º
Direito de não ter dados pessoais utilizados em pesquisa sobre saúde pública transferidos a terceiros pelo órgão de pesquisa	Art. 13, § 2º
Direito ao término do tratamento, quando verificado que: (i) a finalidade foi alcançada ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; (ii) houve o fim do período de tratamento; (iii) houve comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, conforme disposto no § 5º do art. 8º da Lei e resguardado o interesse público; ou (iv) por determinação da autoridade nacional, quando houver violação ao disposto na Lei	Art. 15
Direito à eliminação ou ao apagamento dos dados, no âmbito e nos limites técnicos das atividades, sendo autorizada a conservação somente nas exceções legais	Art. 16

1.3 EXERCÍCIO DOS DIREITOS DOS TITULARES PERANTE A ADMINISTRAÇÃO

Para o exercício dos direitos dos titulares, a Lei prevê um conjunto de ferramentas, que, no âmbito público, traduzem-se em mecanismos que aprofundam obrigações de transparência ativa e passiva, bem como criam meios processuais para provocar a Administração Pública.

Essas obrigações são apresentadas neste documento como: (i) obrigações de transparência ativa [que serão tratadas no item 2.4, denominado Publicidade]; (ii) meios de acesso à informação em transparência passiva; e (iii) meios de petição e manifestação à administração pública.

Em todos os casos, o titular do dado tem a faculdade de optar por resposta por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa.

1.3.1 Meios de acesso à informação em transparência passiva

Parte substancial dos direitos dos titulares perante o poder público são exercidos por meio do exercício do direito de acesso à informação. É sempre importante salientar que a Lei 12.527/2011, a LAI, já previa, em seu art. 31, procedimentos e diretrizes básicas para o tratamento de dados pessoais no âmbito público. Entre eles, estão o tratamento transparente, a garantia expressa aos direitos de personalidade e o consentimento do titular para a disponibilização de suas informações àqueles que não possuíssem a necessidade de conhecê-la no exercício de sua função pública. Aquela Lei chegou a prever, inclusive, regulamentação específica para o tratamento de dados pessoais no âmbito público.

A LGPD, reconhecendo esse legado, informa que, no âmbito público, os prazos e procedimentos para o exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, citando (mas sem se ater exclusivamente) a Lei de Acesso à Informação, a Lei do Processo Administrativo e a Lei do Habeas data (essa última no âmbito judicial).

Desta forma, submetem-se aos prazos e procedimentos já estabelecidos pela Lei nº 12.527/2011 - inclusive com o recebimento dos requerimentos junto ao Serviço de Informação ao Cidadão - o exercício dos seguintes direitos expressamente previstos na Lei Geral de Proteção de Dados Pessoais:

a. acesso à informação sobre a confirmação da existência de tratamento (art. 18, I);

b. acesso aos dados coletados (art. 18, II);

c. acesso à informação sobre entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (art. 18, VII);

d. nos casos em que o tratamento tiver origem no consentimento do titular ou em contrato, o acesso à cópia eletrônica integral de seus dados pessoais. Devem ser observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente inclusive em outras operações de tratamento (art. 19, §3º); e

e. acesso às informações a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial (art. 20, §1º).

1.3.2 Meios de petição e manifestação à administração pública

Como já mencionado, no âmbito administrativo, a LGPD cita expressamente as Leis 12.527/2011 (LAI) e 9.784/1999 (processo administrativo) como referência não exclusiva para o exercício dos direitos dos titulares. É de se repisar que, ao mesmo tempo, ela aparta os procedimentos que ela prevê daqueles a serem utilizados em face do poder público, ao mencionar que o exercício de tais direitos seria realizado por meio de legislação específica.

Como a Lei não estabelece a observância exclusiva daquele conjunto da Lei de Acesso à Informação e da Lei Geral do Processo Administrativo, e considerando a existência de procedimentos mais benéficos ao titular para o exercício de seus direitos no que se refere a esse último conjunto apresentado, **o mecanismo mais célere estabelecido pelo Código de Defesa dos Usuários de Serviços Públicos (Lei n° 13.460/2017) poderia ser adotado como padrão para o recebimento**

de solicitações de providências e reclamações relativas ao tratamento de dados. Além da vantagem em termos de prazo e procedimentos padronizados, com unidades de recebimento de petições e reclamações padronizadas e coordenadas, a Lei 13.460/2017, diferentemente da Lei Geral do Processo Administrativo, tem abrangência nacional, permitindo melhor coordenação entre instituições públicas na defesa dos direitos dos titulares de dados.

O titular do dado tem o direito, mediante requerimento expresso seu ou de representante legalmente constituído, sem custos, nos prazos e nos termos previstos em regulamento, de requisitar manifestação conclusiva do controlador ou agente responsável pelo tratamento sobre os seguintes itens:

a. correção de dados incompletos, inexatos ou desatualizados (art. 18, III);

b. anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD (art. 18, IV);

c. eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD (art. 18, VI); e

d. revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (art. 20).

A resposta deve ser providenciada de imediato e em formato simplificado; ou por declaração clara e completa, fornecida no prazo previsto em Lei e que indique: origem dos dados, a inexistência de registro, critérios utilizados, finalidade do tratamento (observados os segredos comercial e industrial).

O titular do dado tem a faculdade de optar por resposta por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa.

A petição deve ser respondida com agilidade, clareza e completude, sob pena de o titular dos dados ter a prerrogativa de representar contra o responsável na ANPD, organismos de defesa do consumidor ou ajuizar pretensão com tal causa de pedir.

Na impossibilidade de atendimento imediato do requerimento do titular do dado pessoal, o controlador poderá comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

Por último, o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Nas hipóteses acima, o controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. Quando tais segredos impossibilitarem o oferecimento de informações, a ANPD poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Os dados pessoais referentes ao exercício regular de direitos pelo titular, previstos no Art. 18 da LGPD (Capítulo III), não podem ser utilizados em seu prejuízo. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

1.4 TIPOLOGIA DE DADOS PESSOAIS

No âmbito da administração pública federal, nos habituamos ao uso de um conjunto de terminologias decorrentes da implantação da LAI (Lei nº 12.527/2011), tais como “informação

pessoal" e "informação pessoal sensível". A fim de que possamos harmonizar os conceitos até então replicados naquele contexto com aqueles trazidos pela LGPD e pelo Decreto nº 10.046/2019, relembremos o modo como os utilizamos ao longo dos últimos anos.

De acordo com o inciso IV do artigo 4˚ da Lei n˚ 12.527/11, informação pessoal é aquela relacionada à pessoa natural identificada ou identificável. Entende-se por pessoa natural a pessoa física, ou seja, o indivíduo. Os contornos mais relevantes desse conceito são apresentados pelo artigo 31 da LAI, o qual foi regulamentado pelos artigos 55 a 62 do Decreto nº 7.724/12.

Segundo o art. 31 da LAI, não é toda e qualquer informação pessoal que goza de um regime específico de proteção. Apenas aquela com potencial de vulnerar os direitos de personalidade, tais como definidos no art. 5º, X da Constituição Federal, estaria sob uma proteção especial. No núcleo desse conjunto de dados, estaria o que se denominou, com amparo na doutrina existente, a informação pessoal sensível. Ou seja, aquela informação que viola o direito de autodeterminação da imagem ou que possa levar a que terceiros adotem ações discriminatórias contra o titular daquele dado. A existência de gradações desta natureza mostrou-se bastante importante ao longo dos últimos anos, pois passou a indicar limites à mitigação da expectativa de privacidade no caso em que os titulares dos dados eram os próprios agentes públicos.

A LGPD manteve o conceito de dado pessoal trazido pela Lei 12.527/2011 e evoluiu sobre o conceito de informação sensível: **"dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural"** (Art. 5º, II).

Diferentemente da LAI, no entanto, os direitos e salvaguardas sobre dados pessoais da LGPD incidem sobre todos os tipos de dados pessoais, observadas as legislações existentes, inclusive os regimes existentes de transparência e acesso à informação. Ou seja, a tutela da lei se estende não mais apenas aos dados pessoais sensíveis ou diretamente relacionados aos direitos de personalidade, mas, em maior ou menor medida, a todos os dados pessoais.

Com a edição do Decreto nº 10.046/2019, buscou-se agrupar essas categorias em uma matriz que torna mais racional a gestão de informações pelos órgãos e entidades públicas. Desta forma, à taxonomia de dados pessoais já existente, soma-se o que se denomina (i) atributos biográficos; (ii) atributos biométricos; (iii) atributos genéricos; e (iv) dados cadastrais, assim definidos:

> (i) atributos biográficos - dados de pessoa natural relativos aos fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios;
>
> (ii) atributos biométricos - características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, conforme Art. 2º, inciso II do Decreto 10.046/2019;
>
> (iii) atributos genéticos - características hereditárias da pessoa natural, obtidas pela análise de ácidos nucleicos ou por outras análises científicas; e
>
> (iv) dados cadastrais - informações identificadoras perante os cadastros de órgãos públicos.

Não existe uma perfeita coincidência entre tais atributos e os conceitos que vimos até agora; porém, a compatibilização destes conceitos é bastante simples.

Primeiramente, **cabe destacar que todos os tipos de atributos constituem informações pessoais, pois são relativos a titular pessoa física identificado ou identificável.**

Atributos genéticos e biométricos, por definição legal, constituem dados pessoais sensíveis. Atributos biográficos, em conjunto com dados como números de cadastro tais como CPF, CNPJ, NIS, PIS, PASEP e Título de Eleitor são o que se denomina de dados cadastrais.

Por sua vez, a depender do seu conteúdo, atributos biográficos poderão ou não ser considerados sensíveis. Nos termos da Lei, serão considerados sensíveis aqueles atributos biográficos que digam respeito à convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político.

Assim, via de regra, o tratamento de atributos biométricos e genéticos se dará com base no regime de tratamento de dados pessoais sensíveis; já o tratamento de atributos biográficos será feito de acordo com o seu conteúdo, o qual definirá a tipologia do dado à luz da LGPD.

2 COMO REALIZAR O TRATAMENTO DOS DADOS PESSOAIS

2.1 HIPÓTESES DE TRATAMENTO

A LGPD autoriza, em seu art. 23, os órgãos e entidades da administração pública a realizar o tratamento de dados pessoais unicamente para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que as hipóteses de tratamento sejam informadas ao titular.

Como visto, o tratamento de dados pessoais poderá ser realizado desde que enquadrado em uma das hipóteses elencadas em seu art. 7º. Tais hipóteses podem ser compreendidas como condições necessárias para verificar se o tratamento de dados a ser realizado pelo controlador ou operador é permitido.

A seção 1 deste documento descreve as hipóteses de tratamento de dados autorizadas pela LGPD. É necessário que os órgãos e entidades da APF conheçam todas as hipóteses para:

- Analisar os casos de tratamento de dados pessoais já realizados, objetivando verificar se há hipótese legal que os autorize; e

- Avaliar previamente cada novo caso de tratamento que pretenda realizar, identificando as hipóteses legais autorizativas aplicáveis.

A tabela a seguir elenca resumidamente as hipóteses de tratamento autorizadas pela LGPD.

Tabela 3 Hipóteses de tratamento de dados pessoais

HIPÓTESE DE TRATAMENTO	DISPOSITIVO LEGAL	REQUER CONSENTIMENTO DO TITULAR?
Hipótese 1: Mediante consentimento do titular	LGPD, art. 7º, inciso I	Sim
Hipótese 2: Para o cumprimento de obrigação legal ou regulatória	LGPD, art. 7º, inciso II	Não
Hipótese 3: Para a execução de políticas públicas	LGPD, art. 7º, inciso III	Não
Hipótese 4: Para a realização de estudos e pesquisas	LGPD, art. 7º, inciso IV	Não
Hipótese 5: Para a execução ou preparação de contrato	LGPD, art. 7º, inciso V	Termos de consentimento definidos no contrato ou decorrentes da autonomia da vontade.

Hipótese 6: Para o exercício de direitos em processo judicial, administrativo ou arbitral	LGPD, art. 7º, inciso VI	Não
Hipótese 7: Para a proteção da vida ou da incolumidade física do titular ou de terceiro	LGPD, art. 7º, inciso VII	Não
Hipótese 8: Para a tutela da saúde do titular	LGPD, art. 7º, inciso VIII	Não
Hipótese 9: Para atender interesses legítimos do controlador ou de terceiro	LGPD, art. 7º, inciso IX	Não
Hipótese 10: Para proteção do crédito	LGPD, art. 7º, inciso X	Não

A LGPD estabelece também, em seu art. 6º, que o tratamento de dados pessoais deve observar a boa-fé e dez princípios fundamentais específicos. São eles:

- finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
- transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e
- responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Não basta, portanto, o enquadramento em uma das hipóteses legais autorizativas para se iniciar o tratamento de dados pessoais. É fundamental garantir que os princípios listados acima sejam respeitados.

Nesse sentido, no intuito de auxiliar os órgãos e entidades da APF no processo de adequação à LGPD, foram elaborados checklists que destacam questões fundamentais a serem verificadas para garantir a conformidade do tratamento de dados pessoais às disposições da Lei.

Os checklists poderão ser utilizados tanto no início de novos tratamentos, quanto na avaliação da conformidade de tratamentos iniciados antes da vigência da LGPD.

2.1.1 Identificação das hipóteses de tratamento aplicáveis

Como determinar a hipótese legal que autoriza o tratamento de dados pessoais? Isso depende das finalidades e contextos específicos de cada situação.

É natural imaginar que, para órgãos e entidades públicas, seriam sempre aplicáveis as hipóteses 2 e 3 da Tabela 3, quais sejam: "Para o cumprimento de obrigação legal ou regulatória" e "Para a execução de políticas públicas". No entanto, não existe um caso geral que se adeque a todas as situações, mesmo considerando tratar-se de órgãos e entidades públicas. Poderá haver inclusive situações em que mais de uma hipótese legal seja cabível, se houver múltiplos propósitos para o tratamento do dado.

O importante é avaliar caso a caso e documentar a(s) hipótese(s) aplicável(is), uma vez que o titular deverá conhecer a hipótese legal que autoriza o processamento de seus dados pessoais.

Além disso, o princípio da responsabilização e prestação de contas requer que o órgão ou entidade que realiza o tratamento de dados pessoais possa demonstrar que está plenamente aderente à LGPD, comprovando a observância e o cumprimento das normas de proteção de dados pessoais estabelecidas, inclusive quanto a sua eficácia.

Por essa razão, cabe ao órgão ou entidade pública avaliar bem a hipótese de tratamento aplicável, pois mudanças posteriores podem abalar a confiança do titular quanto aos interesses legítimos da instituição no uso de seus dados, além de comprometer os requisitos de transparência, responsabilização e prestação de contas.

Considerando o exposto acima, reitera-se que foram criados checklists para cada uma das hipóteses de tratamento. Nesses checklists, constam perguntas que objetivam facilitar a identificação da hipótese mais apropriada. Além disso, destacam-se obrigações com as quais o controlador e/ou operador deverá se comprometer ao optar por cada hipótese.

HIPÓTESE 1: Tratamento mediante consentimento do titular

Essa é uma hipótese em que o titular tem chance real de escolha sobre o tratamento de seus dados. Trata-se de hipótese possível quando as demais do art. 7º forem descartadas.

Uma vez descartadas as demais hipóteses, o órgão/entidade deve avaliar:

1. Será viável a coleta e o armazenamento da opção de consentimento do titular de modo a poder comprovar posteriormente a sua expressa manifestação de vontade?

2. Se o consentimento se der de forma escrita, será garantido que a opção pelo consentimento conste de cláusula destacada das demais, em que o titular seja instado a escolher livremente pela anuência ou não ao consentimento solicitado?

3. O consentimento será solicitado para cada uma das finalidades de tratamento, e será informado ao titular que tipo de tratamento será realizado, antes que este opte pelo consentimento?

Observações:

a) É vedado o tratamento de dados pessoais mediante vício de consentimento.

b) O consentimento será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

c) Se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o titular deverá ser informado previamente sobre as mudanças de finalidade, podendo revogar o consentimento, caso discorde das alterações.

d) As autorizações genéricas para o tratamento de dados pessoais serão consideradas nulas.

4. Será dada ao titular a opção de revogação do consentimento, a qualquer momento, mediante manifestação expressa, por procedimento gratuito e facilitado?

5. No caso de tratamento de dados de crianças e adolescentes, será solicitado o consentimento específico por pelo menos um dos pais ou pelo responsável legal?

Ressalta-se que todas as questões acima, se aplicáveis, devem ser respondidas positivamente para que a hipótese de tratamento do dado por consentimento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 2: Tratamento para o cumprimento de obrigação legal ou regulatória

Essa hipótese é aplicável quando é necessário processar dados pessoais para o cumprimento de obrigações legais ou regulatórias específicas. Não se enquadram nessa hipótese as obrigações estabelecidas por contrato.

Para enquadramento nessa hipótese, deve-se avaliar:

1. É possível identificar a obrigação legal ou regulatória específica que requer o processamento do dado?

2. O titular do dado será informado sobre a norma que determina a obrigação legal ou regulatória que exige o tratamento do dado?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 3: Tratamento para a execução de políticas públicas

Essa hipótese é aplicável para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. Trata-se de uma hipótese que dispensa o consentimento do titular e que deve ser realizada por controladores que sejam pessoas jurídicas de direito público.

Os controladores podem, no entanto, envolver operadores para a realização do tratamento de dados pessoais necessários à consecução de políticas públicas. Estes últimos podem ser pessoas jurídicas de direito privado.

Para enquadramento nessa hipótese, deve-se avaliar:

1. O controlador é pessoa jurídica de direito público?

2. Não sendo pessoa jurídica de direito público, o controlador é empresa pública ou sociedade de economia mista que realizará o tratamento de dados para execução de políticas públicas, e não para atividades inerentes ao regime de concorrência?

3. O tratamento do dado será realizado para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres?

4. É possível identificar claramente a lei, regulamento ou outro instrumento legal que especifique a política pública que exige o tratamento de dados pessoais?

5. O titular do dado será informado sobre a lei, regulamento ou outro instrumento legal que especifique a política pública que exige o tratamento do dado?

6. Será indicado um encarregado para garantir a comunicação do órgão ou entidade pública com o titular do dado e com a Autoridade Nacional de Proteção de Dados, que verificará a observância das instruções e normas sobre a política pública em questão?

O Art. 5º, inciso VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

Segundo o Art. 23 da LGPD, os órgãos e entidades públicas deverão realizar o tratamento de dados apenas para o atendimento de sua finalidade pública, na persecução do interesse público e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Nesse contexto, não havendo uma delimitação inequívoca das atribuições legais que poderiam ser diretamente relacionadas à execução de políticas públicas, cabe aos órgãos e entidades analisar, no caso concreto, a possibilidade enquadrar o tratamento do dado na hipótese prevista no Art. 7º, inciso III, combinada com o disposto no Art. 23.

HIPÓTESE 4: Tratamento para a realização de estudos e pesquisas

Essa hipótese é aplicável para o tratamento de dados para realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

Para enquadramento nesta hipótese, deve-se avaliar:

1. O controlador ou operador é órgão de pesquisa?
2. Os dados pessoais serão utilizados dentro do órgão estritamente para a finalidade estabelecida para o estudo ou pesquisa?
3. Em se tratando de estudos em saúde pública, os dados serão mantidos em ambiente seguro e controlado, e será garantida, sempre que viável, a anonimização ou pseudonimização dos dados?
4. O órgão de pesquisa garante que não serão revelados dados pessoais em caso de divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa realizada?
5. O órgão de pesquisa que tiver acesso aos dados pessoais assume a responsabilidade pela segurança da informação e se compromete a não transferir os dados a terceiros em circunstância alguma?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 5: Tratamento para a execução de contrato ou de procedimentos preliminares relacionados a contrato

Essa hipótese é aplicável para o tratamento de dados necessário à execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular. As hipóteses de tratamento de dados estarão previstas no contrato. O consentimento é fornecido no ato de formalização do termo ou decorrente do mesmo.

Para enquadramento nessa hipótese, deve-se avaliar:

1. O tratamento de dados pessoais se faz necessário para a consecução dos termos do contrato ou para a realização de procedimentos preliminares relacionados ao contrato?

Essa pergunta deve ser respondida positivamente para que tal hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 6: Tratamento para o exercício de direitos em processo judicial, administrativo ou arbitral

Essa hipótese é aplicável para o tratamento de dados necessário ao exercício regular de direitos do titular em processo judicial, administrativo ou arbitral, por quaisquer das partes envolvidas.

Para enquadramento nessa hipótese, deve-se avaliar:

1. O tratamento de dados pessoais se faz necessário para o exercício de direitos do titular em processo judicial, administrativo ou arbitral?

2. O titular do dado será informado com destaque quando essa hipótese de tratamento for aplicada?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 7: Tratamento para a proteção da vida ou da incolumidade física do titular ou de terceiro

Essa hipótese é aplicável para o tratamento de dados para a proteção da vida ou da incolumidade física do titular ou de terceiro.

Para enquadramento nessa hipótese, deve-se avaliar:

1. O tratamento de dados pessoais se faz necessário para proteger a vida ou a incolumidade física do titular ou de terceiro?

2. O titular está impossibilitado de oferecer o consentimento para o tratamento do dado pessoal?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 8: Tratamento para a tutela da saúde do titular

Essa hipótese é aplicável para o tratamento de dados para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Para enquadramento nessa hipótese, deve-se avaliar:

1. O tratamento de dados pessoais será realizado por profissional de saúde, serviço de saúde ou autoridade sanitária?

2. O tratamento de dados pessoais se faz necessário para a tutela da saúde do titular?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 9: Tratamento para atender interesses legítimos do controlador ou de terceiro

Essa hipótese é aplicável para o tratamento de dados quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Órgãos e entidades públicas não devem recorrer a essa hipótese se o tratamento de dados ocorre para a consecução de políticas públicas ou de suas próprias competências legais. No entanto, em caso de finalidade diversa, essa opção poderá ser aplicável.

Para enquadramento nessa hipótese, deve-se avaliar:

1. Foi identificado interesse legítimo do controlador, considerado a partir de situações concretas, que respeite as legítimas expectativas do titular em relação ao tratamento de seus dados?

2. O controlador se responsabiliza por garantir a proteção do exercício regular dos direitos do titular ou a prestação de serviços que o beneficiem, respeitados os direitos e liberdades fundamentais do titular?

3. O titular do dado será comunicado sobre a hipótese de tratamento de dados aplicada?

4. Serão adotadas medidas para garantir a transparência do tratamento de dados baseado no legítimo interesse do controlador?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

HIPÓTESE 10: Tratamento para proteção do crédito

Essa hipótese é aplicável para o tratamento de dados para proteção do crédito do titular.

Para enquadramento nessa hipótese, deve-se avaliar:

1. Foi identificada necessidade de tratamento de dados pessoais para a proteção do crédito do titular?

2. O titular do dado será comunicado sobre a hipótese de tratamento de dados aplicada?

As questões acima devem ser respondidas positivamente para que essa hipótese de tratamento seja aplicável e para a garantia de que o tratamento se dará em estrita observância à LGPD.

2.1.2 Verificação de conformidade do tratamento de dados quanto aos princípios da LGPD

Uma vez identificada(s) a(s) hipóteses de tratamento aplicável(is) às situações específicas de processamento de dados por órgãos e entidades da Administração Pública Federal, deve-se partir para outras questões importantes para a verificação da conformidade quanto aos princípios da LGPD.

Para tanto, o órgão ou entidade pública deverá analisar outras questões, detalhadas a seguir.

1. Identifique a finalidade para a qual o tratamento de dado é necessário. Os propósitos devem ser legítimos, específicos e explícitos (princípio da finalidade).

2. Defina como a finalidade do tratamento será informada ao titular, o que deve ser realizado antes do início do tratamento do dado (princípio da finalidade).

3. No caso de tratamento de dados que tenha sido iniciado antes da vigência da Lei, indique que providências serão tomadas para comunicar o titular sobre o tratamento realizado e a finalidade a qual se destina (princípio da finalidade).

4. Garanta que o tratamento do dado será apenas para a finalidade informada ao titular (princípio da adequação). Quaisquer mudanças na finalidade de tratamento deverão ser também comunicadas ao titular do dado.

5. Ao planejar a forma de tratamento de dados, atente para limitar a utilização ao mínimo de informações necessárias, garantindo abrangência pertinente e proporcional à consecução das finalidades informadas ao titular (princípio da necessidade).

6. Ao decidir realizar o tratamento de dados, defina antecipadamente os mecanismos e procedimentos que os titulares dos dados deverão utilizar para consultar o conteúdo, a forma e a duração do tratamento dos seus dados pessoais, de maneira facilitada e gratuita (princípio do livre acesso).

7. Garanta que quaisquer alterações quanto à finalidade especificada para o tratamento do dado; à forma ou à duração do tratamento; ao controlador responsável pelo dado; ou, ainda, à abrangência de compartilhamento sejam comunicadas ao titular (princípio do livre acesso).

8. Defina procedimento de verificação contínua quanto à exatidão, à clareza, à relevância e à atualização dos dados do titular. O objetivo é manter-se fiel à finalidade de tratamento informada (princípio da qualidade do dado).

9. Observe a necessidade de garantir ao titular a opção de obter facilmente informações claras e precisas, mediante requisição, sobre o tratamento que é dado a seus dados e sobre os respectivos agentes de tratamento (princípio da transparência).

Observação:

Os órgãos / entidades deverão garantir o acesso às informações sobre o tratamento do dado do titular, resguardadas as informações de acesso restrito, conforme legislação vigente. Vide item 2.4, sobre publicidade.

10. Defina e documente as medidas técnicas e administrativas que serão adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (princípio da segurança).

11. Identifique e registre as medidas que serão adotadas para prevenir a ocorrência de danos ao titular ou a terceiros em virtude do tratamento de dados pessoais (princípio da prevenção).

12. Comprometa-se a não realizar o tratamento do dado para fins discriminatórios ilícitos ou abusivos (princípio da não discriminação).

13. Comprometa-se a adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais (princípio da responsabilização e prestação de contas).

Para iniciar novos tratamentos de dados, é fundamental que os órgãos e entidades da APF analisem todas as questões citadas acima e documentem a forma de aplicação de cada um dos

princípios da LGPD. O Relatório de Impacto à Proteção de Dados Pessoais – RIPD representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição. Serve tanto para a análise quanto para a documentação. Na seção 2.5 constam orientações no sentido de auxiliar os órgãos e entidades a elaborar um RIPD.

A análise das questões acima deve também ser realizada para os casos de tratamento de dados anteriores à vigência da Lei. Nesses casos, é importante identificar os pontos de não conformidade com a LGPD, para os quais deverão ser elaborados planos para adaptação à Lei.

2.1.3 Especificidades para o tratamento de dados pessoais sensíveis

A LGPD traz regramento específico para o tratamento de dados pessoais sensíveis, que são definidos no art. 5º, inciso II como "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

São dados cujo tratamento pode ensejar a discriminação do seu titular, e por isso, são sujeitos a proteção mais rígida.

O art. 11 da LGPD elenca as hipóteses em que o tratamento de dados pessoais sensíveis pode ser realizado. Novamente, a lei traz a possibilidade de tratamento mediante consentimento do titular, como regra, e enumera as hipóteses que dispensam o consentimento, por meio de rol extensivo.

O tratamento mediante consentimento exige que se registre a manifestação de vontade do titular de forma específica e destacada, dando ciência do conhecimento sobre as finalidades específicas daquele tratamento.

Já o tratamento de dados pessoais sensíveis sem o fornecimento de consentimento do titular somente pode ocorrer nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (resguardados os direitos do titular mencionados no art. 9º da Lei sobre o acesso facilitado às informações quanto ao tratamento dos seus dados. A exceção a este item é no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais).

Observa-se que os órgãos e entidades da administração pública federal poderão enquadrar-se em diversas hipóteses de dispensa de consentimento para o tratamento de dados de pessoais sensíveis. No entanto, cabe destacar que a lei determina o tratamento desse tipo de dado apenas em **situações indispensáveis**. Isso traz para o controlador o ônus da prova da alegada indispensabilidade.

Os órgãos e entidades públicas que realizarem o tratamento dos dados pessoais sensíveis deverão dar publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 da Lei.

Especificamente no que tange à realização de estudos em saúde pública, o art. 13 da Lei possibilita que os órgãos tenham acesso a bases de dados pessoais, inclusive os atributos sensíveis, que serão tratados exclusivamente dentro do referido órgão e estritamente para a finalidade de

realização de estudos e pesquisas. Nessa hipótese, o órgão ou entidade deverá garantir que os dados sejam mantidos em ambiente controlado e seguro, e que, sempre que possível, sejam anonimizados ou pseudonimizados (vide Seção 2.3).

A LGPD traz ressalva expressa à divulgação de dados pessoais quando da publicação de resultados ou de qualquer excerto de estudo ou de pesquisa realizada.

2.1.4 Especificidades para o tratamento de dados de crianças e adolescentes

Assim como para o caso das informações pessoais sensíveis, a LGPD dedica também atenção especial ao tratamento de dados de crianças e adolescentes.

A Lei determina, em seu art. 14, que o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, mediante consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. Nessa hipótese, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para acesso às informações tratadas.

É também dever do controlador envidar todos os esforços razoáveis para verificar se o consentimento foi dado realmente pelo responsável pela criança, consideradas as tecnologias disponíveis. **Esse é, portanto, o desafio na coleta de dados pessoais de crianças e adolescentes, pois o consentimento é exigido inclusive no caso de execução de políticas públicas**, o que não ocorre com adultos.

A única hipótese que dispensa o consentimento mencionado acima ocorre quando a coleta for necessária para contatar os pais, ou o responsável legal, ou, ainda, para a própria proteção da criança ou adolescente. Nesses casos, os dados deverão ser utilizados uma única vez, vedados o armazenamento e o seu repasse a terceiros.

Contudo, a hipótese de coleta de consentimento dos pais ou responsáveis não se confunde com situações nas quais o tratamento do dado é necessário para o exercício de direitos da criança ou adolescente ou para lavratura de registros públicos.

Caso os órgãos e entidades públicas desenvolvam jogos, aplicações de internet ou outras atividades semelhantes voltadas ao público infanto-juvenil, a coleta de dados pessoais dos jovens deverá restringir-se ao estritamente necessário à atividade proposta.

2.2 COLETA

A coleta é uma das operações de tratamento referenciadas pelo art. 5º, inciso X da LGDP. Considerando que o tratamento de dados pode ser representado por um ciclo de vida, essa operação representa a etapa inicial responsável por obter os dados pessoais do cidadão (titular dos dados). A representação do tratamento de dados pessoais como ciclo de vida é tratada no capítulo 3 deste documento.

Tendo em vista que a coleta é a operação inicial de tratamento dos dados pessoais, a realização de tal operação pela instituição somente deve ser realizada mediante o atendimento das hipóteses de tratamento, das medidas de segurança, dos princípios, dos diretos do titular e demais regras dispostas pela LGPD.

Todo o conteúdo deste documento visa justamente orientar as instituições para os cuidados que elas devem ter ao coletar e tratar os dados pessoais dos cidadãos de forma a assegurar a privacidade dos titulares de dados. A seção 4.1.2 orienta sobre a incorporação da privacidade como padrão para o tratamento dos dados pessoais, indicando a limitação da coleta como uma das práticas a serem adotadas.

2.3 ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

Segundo a LGPD, **dado anonimizado é o dado relativo a titular que não possa ser identificado.** A não identificação da relação entre o dado e seu proprietário decorre da utilização da técnica de anonimização, a fim de impossibilitar a associação entre estes, seja de forma direta ou indireta.

É importante ressaltar que, ainda que o dado esteja anonimizado, uma vez observada a possibilidade de reversão do processo que obteve a anonimização, este processo deixa de ser assim considerado e passa a ser considerado **pseudonimização**. Esses processos, de acordo com a legislação em vigor, devem ser utilizados, sempre que possível, por meio da aplicação de meios técnicos razoáveis e disponíveis na ocasião do tratamento dos dados.

A seguir, algumas recomendações para subsidiar a escolha da técnica a ser utilizada:

- Elencar os principais processos de trabalho que realizam tratamento de dados pessoais para a realização de estudos, especialmente em órgão de pesquisa, conforme Art. 7º, IV.
- Identificar os dados pessoais a que se referem os processos de trabalho listados, que não podem ter os proprietários relacionados.
- Analisar o ciclo de vida de tratamento do dado a fim de mitigar riscos de violação de dados que não são mais de uso corrente. E, ainda, propor arquivamento ou eliminação dos dados, visto que a gestão de dados desnecessários no ambiente de produção causa aumento não apenas do quantitativo de dados a serem geridos, como também a manutenção do custo operacional relacionado a este processo (em atividades como armazenamento e gestão da segurança).
- Avaliar o risco de identificação do titular dos dados listados. Deve-se levar em consideração que, quanto maior o uso de tecnologias de análise de dados, quanto maior o volume de dados processados e quanto mais sensíveis forem estes dados, maior será o risco de violação.
- Quando houver a obrigatoriedade de proteção de dados pessoais, sem a necessidade de guarda dos dados que associam estes aos proprietários, pode-se optar pelo processo de anonimização, sem prejuízo de atividades do órgão ou entidade. Caso contrário, pode-se optar pela técnica de pseudonimização.
- Definir um plano de comunicação para incidentes de violação de dados. O objetivo é propiciar maior celeridade na solução de incidentes e padronização de atividades a serem executadas, assim como prever responsáveis pelo cumprimento das atividades.
- Documentar violações atestadas e incidentes ocorridos, a fim de analisar riscos de violação periodicamente.
- Promover a conscientização contínua acerca da importância da proteção de dados no órgão ou entidade.

Cabe destacar que a pseudonimização é uma técnica utilizada para proteção de dados pessoais. Pode ser utilizada, por exemplo, para preservação da identidade do denunciante, conforme previsto no §4º do art. 6º do Decreto nº 10.153/2019.

> Art. 6º O denunciante terá seus elementos de identificação preservados desde o recebimento da denúncia, nos termos do disposto no § 7º do art. 10 da Lei nº 13.460, de 2017.
>
> § 4º A unidade de ouvidoria responsável pelo tratamento da denúncia providenciará a sua **pseudonimização** para o posterior envio aos órgãos de apuração competentes, observado o disposto no § 2º.

A pseudonimização também pode ser utilizada para proteger a identidade do usuário de serviço público ou autor de manifestação conforme previsão do art. 24 do Decreto nº 9.492/2018.

> Art. 24. As unidades que compõem o Sistema de Ouvidoria do Poder Executivo federal assegurarão a proteção da identidade e dos elementos que permitam a identificação do usuário de serviços públicos ou do autor da manifestação, nos termos do disposto no art. 31 da Lei nº 12.527, de 18 de novembro de 2011.

2.4 PUBLICIDADE

O inciso I do art. 23 da LGPD impõe às pessoas jurídicas de direito público obrigações de transparência ativa. Isto é, de **publicar informações sobre os tratamentos de dados pessoais por elas realizados em seus sítios eletrônicos de forma clara e atualizada, detalhando a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução desses tratamentos.**

Também deve ser dada **publicidade aos tratamentos de dados pessoais sensíveis** em que seja dispensado o consentimento do titular, seja para cumprimento de obrigação legal ou regulatória, seja para tratamento compartilhado de dados necessários para a execução de políticas públicas previstas em leis ou regulamentos, conforme prevê o §2º do art. 11 da LGPD.

Outra informação a ser publicizada é a identidade e informações de contato do encarregado, por força do art. 41, §1º da LGPD.

Quando o tratamento de dados pessoais envolver a obrigação legal de difusão destes em transparência ativa, estes devem ser publicados em formato interoperável e estruturado para o uso compartilhado, em cumprimento ao disposto no art. 25 da LGPD e como já previa o art. 8º, §3 da Lei nº 12.527/2011, a Lei de Acesso à Informação.

Quanto à localização da publicação das informações sobre o tratamento de dados pessoais, sensíveis ou não, sugere-se que, além dos itens especificados para serem publicados em seção específica denominada "Acesso à Informação" dos sítios eletrônicos dos órgãos pelo "Guia de Transparência Ativa (GTA) para os órgãos e entidades do Poder Executivo Federal", publicado pela Controladoria-Geral da União, seja incluído o item "Tratamento de Dados Pessoais". O GTA está disponível em: <<http://www.acessoainformacao.gov.br/lai-para-sic/guias-e-orientacoes/gta-6a-versao-2019.pdf/view>>.

Sugere-se como texto de introdução: "Nesta seção, são divulgadas informações sobre o tratamento de dados pessoais realizado pelo(a) [nome do órgão ou entidade], compreendendo a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução desse tratamento, em cumprimento ao disposto no inciso I do art. 23 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD)".

Em seguida, devem ser publicadas as seguintes informações sobre o encarregado:

DADOS DO ENCARREGADO (art. 41 da LGPD)

I. Nome e cargo do encarregado indicado pelo controlador;

II. Localização;

III. Horário de atendimento;

IV. Telefone e e-mail específico para orientação e esclarecimento de dúvidas.

Neste item, deve ser publicado, ainda, banner para o **Fala.BR**, que será o canal para endereçamento de petições e reclamações do titular de dados, previsto nos artigos 18 e 20 da LGPD.

A seguir, devem ser publicados nessa seção versões resumidas dos Relatórios de Impacto à Proteção de Dados Pessoais - RIPD (ver seção seguinte deste documento). Os relatórios devem contemplar o fornecimento das informações sobre previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dos tratamentos de dados pessoais.

Além de divulgação na seção de "Acesso à Informação" na página eletrônica do órgão, a informação sobre o tratamento de dados pessoais e a finalidade devem ser informadas na descrição do serviço no portal **gov.br**. Na descrição do serviço é importante também destacar quais são os dados pessoais utilizados pelo órgão e a base legal ou a política pública que respalda a obtenção de tais dados.

2.5 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

2.5.1 O que é o Relatório de impacto à proteção de dados pessoais

O **Relatório de Impacto à Proteção dos Dados Pessoais (RIPD)** representa documento fundamental a fim de demonstrar os dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados.

Segundo o inciso XVII do art. 5º da LGPD, o RIPD é documentação que deve ser mantida pelo **Controlador** dos dados pessoais.

> Art. 5º Para os fins desta Lei, considera-se:
>
> **XVII - relatório de impacto à proteção de dados pessoais:** documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

Enquanto o art. 5º inciso XVII define o que é um **RIPD**, o seu conteúdo mínimo é indicado pelo parágrafo único do art. 38, grifado abaixo.

> **Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais**, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
>
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

As próximas seções descrevem o processo de elaboração do RIPD, cujo modelo completo encontra-se no Anexo I.

O formulário de **RIPD** apresentado neste instrumento de orientação constitui uma sugestão para auxiliar os órgãos e entidades na documentação da avaliação de impacto sobre dados pessoais. Dessa forma, e caso seja considerado pertinente pela instituição, as seções e o conteúdo do modelo podem ser adaptados para se adequar a cada contexto particular.

2.5.2 Como Elaborar

O **RIPD** deve ser elaborado antes de a instituição iniciar o tratamento de dados pessoais, preferencialmente, na fase inicial do programa ou projeto que tem o propósito de usar esses dados. A elaboração contempla as etapas destacadas pela figura a seguir.

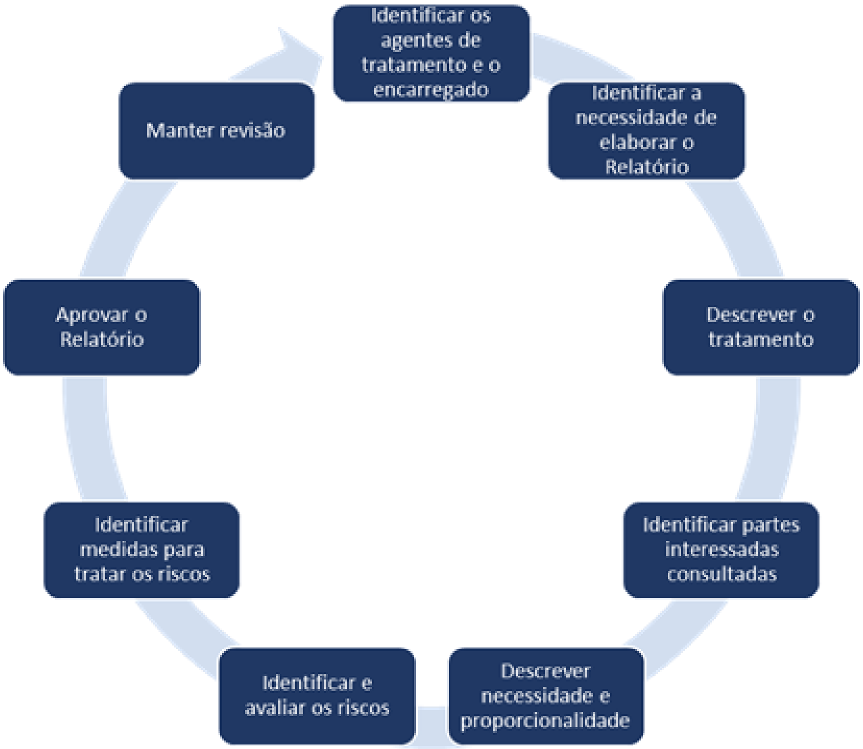


Figura 1 Etapas da Fase de Elaboração do RIPD

2.5.2.1 Identificar os Agentes de Tratamento e o Encarregado

Esta etapa consiste em identificar os agentes de tratamento (controlador e operador) e o encarregado no RIPD (art 5º da LGPD). Esses atores desempenham papel essencial no levantamento das informações necessárias para elaboração do RIPD.

> Art. 5º Para os fins desta Lei, considera-se:
>
> **VI - controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
>
> **VII - operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
>
> **VIII - encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (Redação dada pela Lei nº 13.853, de 2019)

A conclusão desta etapa envolve registrar o e-mail e o telefone de contato do encarregado, já que ele é o canal de comunicação entre o controlador, titulares dos dados e ANPD.

2.5.2.2 Identificar a necessidade de elaborar o Relatório

Inicialmente, é fundamental conhecer os casos específicos previstos pela LGPD em que o RIPD deverá ou poderá ser solicitado. São eles:

- Para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso III do art. 4º);
- Quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 combinados); e
- A qualquer momento sob determinação da ANPD (art. 38).

Quando for necessária a elaboração do **RIPD**, a instituição deve avaliar se os programas, sistemas de informação ou processos existentes ou a serem implementados geram impactos à

proteção dos dados pessoais, a fim de decidir sobre a elaboração ou atualização do **RIPD**.

A elaboração de um único **RIPD** para todas as operações de tratamento de dados pessoais ou de um **RIPD** para cada projeto, sistema, ou serviço deve ser avaliada por cada instituição de acordo com os processos internos de trabalho. Assim, uma instituição que realiza tratamento de quantidade reduzida de dados pessoais, com poucos processos e serviços, pode optar por um **RIPD** único. Já uma instituição que implementa vários processos, projetos, sistemas e serviços que envolvam o tratamento de expressiva quantidade e diversidade de dados pessoais pode considerar que a elaboração de um único **RIPD** não seja a opção mais indicada, optando por elaborar RIPDs segregados por ser mais adequado à sua realidade.

O **Relatório de Impacto** é elaborado ou atualizado sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais, resultante de:

- uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;
- rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada; (LGPD, art. 12 § 2º);
- tratamento de dado pessoal sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (LGPD, art. 5º, II);
- processamento de dados pessoais usado para tomar decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (LGPD, art. 20);
- tratamento de dados pessoais de crianças e adolescentes (LGPD, art. 14);
- tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (LGPD, art. 42);
- tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (LGPD, art. 4º, § 3º);
- tratamento no interesse legítimo do controlador (LGPD, art. 10, § 3º);
- alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados, etc.; e
- reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.

Em síntese, nessa etapa deve(m) ser explicitado(s) qual(is) dos itens elencados acima expressa(m) a necessidade de o **RIPD** ser elaborado ou atualizado pela instituição.

2.5.2.3 Descrever o tratamento

A descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da **natureza, escopo, contexto e finalidade** do tratamento.

Lembrando que a LGPD (art. 5º, X) considera tratamento "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

O objetivo principal desta descrição é fornecer cenário institucional relativo aos processos que envolvem o tratamento dos dados pessoais, fornecendo subsídios para avaliação e tratamento de riscos.

Caso a instituição considere mais adequado para sua realidade de tratamento de dados pessoais, pode-se sintetizar a natureza, escopo, contexto e finalidade do tratamento em uma única seção do RIPD, sem necessidade de segregar a descrição do tratamento em subseções.

2.5.2.3.1 Natureza do tratamento

A **natureza** representa como a instituição pretende tratar ou trata o dado pessoal.

Importante descrever, por exemplo:

- como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;
- fonte de dados (ex: página web, formulário em papel, etc.) utilizada para coleta dos dados pessoais;
- com quais órgãos, entidades ou empresas os dados pessoais serão compartilhados;
- quais são os operadores que realizam o tratamento de dados pessoais em nome do controlador e destacar em quais fases (coleta, retenção, tratamento, distribuição, eliminação) eles atuam;
- se adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais. A informação sobre o uso de nova tecnologia ou método de tratamento é importante no sentido de possibilitar a identificação de possíveis riscos resultantes de tal uso; e
- medidas de segurança atualmente adotadas.

Na elaboração dessa descrição, é importante considerar a possibilidade de consultar um diagrama ou qualquer outra documentação que demonstre os fluxos de dados da instituição.

2.5.2.3.2 Escopo do tratamento

O **escopo** representa a abrangência do tratamento de dados.

Nesse sentido, considerar destacar:

- as informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados são considerados dados pessoais sensíveis.
- o volume dos dados pessoais a serem coletados e tratados;
- a extensão e frequência em que os dados são tratados;
- o período de retenção, informação sobre quanto tempo os dados pessoais serão mantidos, retidos ou armazenados;
- o número de titulares de dados afetados pelo tratamento; e
- a abrangência da área geográfica do tratamento.

O levantamento das informações elencadas acima auxilia a determinar se o tratamento de dados pessoais é realizado em alta escala.

2.5.2.3.3 Contexto do tratamento

Nesta etapa, convém destacar um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas do titular dos dados pessoais ou o impacto sobre o tratamento dos dados.

O levantamento das informações destacadas abaixo proporciona a obtenção de parâmetros que permitirão demonstrar o equilíbrio entre o interesse e a necessidade do controlador em tratar os dados pessoais e os direitos dos titulares de tais dados:

- natureza do relacionamento da organização com os indivíduos;
- nível ou método de controle que os indivíduos exercem sobre os dados pessoais;
- destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável;
- destacar se o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais. Ou seja, o dado pessoal não é tratado de maneira diversa do que é determinado em leis e regulamentos, e comunicado pela instituição ao titular de

dados;

- destaque de qualquer experiência anterior com esse tipo de tratamento de dados;
- destaque de avanços relevantes da instituição em tecnologia ou segurança que contribuem para a proteção dos dados pessoais.

2.5.2.3.4 Finalidade do tratamento

A **finalidade** é a razão ou motivo pelo qual se deseja tratar os dados pessoais. É importantíssimo estabelecer claramente a finalidade, pois é ela que justifica o tratamento e fornece os elementos para informar o titular dos dados.

Nesta etapa, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, considerando os exemplos de finalidades elencadas abaixo, embasados nos artigos 7º e 11 da LGPD, no que for aplicável:

- cumprimento de obrigação legal ou regulatória pelo controlador;
- execução de políticas públicas;
- alguma espécie de estudo realizado por órgão de pesquisa;
- execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- exercício regular de direitos em processo judicial, administrativo ou arbitral;
- proteção da vida ou da incolumidade física do titular ou de terceiro;
- tutela da saúde;
- atender aos interesses legítimos do controlador ou de terceiro;
- proteção do crédito; e
- garantia da prevenção à fraude e à segurança do titular.

Cumpre destacar que os exemplos de finalidades apresentados neste documento não são exaustivos. Desse modo, deve-se informar e detalhar qualquer outra finalidade específica do controlador para tratamento dos dados pessoais, mesmo que tal finalidade não conste dos citados exemplos. Especial atenção deve ser dedicada ao tratamento de dados pessoais realizado com base exclusivamente no consentimento do titular, que pode ocorrer excepcionalmente no caso dos órgãos e entidades públicas. Em ocorrendo, a **finalidade** deve ser precisamente detalhada. Nesse caso, é importante:

- Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados.
- Informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.

Neste momento, deve-se atentar para o caso de a **finalidade** ser para atender o legítimo interesse do controlador. Nesse caso, somente poderá ser fundamentado tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, conforme previsto pelo art. 10 da LGPD.

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
>
> **I - apoio e promoção de atividades do controlador; e**
>
> **II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.**
>
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
>
> § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento

de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Cumpre ressaltar que a instituição deve equilibrar seus interesses com os dos indivíduos com os quais ela tem relacionamento.

2.5.2.4 Identificar partes interessadas consultadas

Partes interessadas relevantes, internas e externas, consultadas a fim de obter opiniões legais, técnicas ou administrativas sobre os dados pessoais que são objeto do tratamento.

Nessa etapa, é importante identificar:

- quais partes foram consultadas, como, por exemplo: operador (LGPD, art. 5º, VII), encarregado (LGPD, art. 5º, VIII), gestores, especialistas em segurança da informação, consultores jurídicos, etc; e
- o que cada parte consultada indicou como importante de ser observado para o tratamento dos dados pessoais em relação aos possíveis riscos referentes às atividades de tratamento em análise. Também deve-se observar os riscos de não-conformidade ante a LGPD e os instrumentos internos de controle (políticas, processos e procedimentos voltados à proteção de dados e privacidade).

Caso não seja conveniente registrar o que foi consultado, então é importante apresentar o motivo de não ter realizado tal registro. Como, por exemplo, apresentar justificativa de que informar o registro das opiniões das partes internas comprometeria segredo comercial ou industrial; fragilizaria a segurança da informação; ou seria desproporcional ou impraticável realizar o registro das opiniões obtidas.

2.5.2.5 Descrever necessidade e proporcionalidade

Descrever como a instituição avalia a necessidade e proporcionalidade dos dados. É necessário demonstrar que as operações realizadas sobre os dados pessoais limitam o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (LGPD, art. 6º, III).

Nesse sentido, destacar:

- A fundamentação legal para o tratamento dos dados pessoais.
- Caso o fundamento legal seja embasado no legítimo interesse do controlador (LGPD, art. 10), demonstrar que:

  - esse tratamento de dados pessoais é indispensável;

  - não há outra base legal possível de se utilizar para alcançar o mesmo propósito; e

  - esse processamento de fato auxilia no propósito almejado.
- Como será garantida a qualidade [exatidão, clareza, relevância e atualização dos dados] e minimização dos dados.
- Quais medidas são adotadas a fim de assegurar que o operador (LGPD, art. 5º, VII) realize o tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pela instituição que exerce o papel de controlador (LGPD, art. 5º, VI).
- Como estão implementadas as medidas que asseguram o direito do titular dos dados pessoais obter do controlador o previsto pelo art. 18 da LGPD.
- Como a instituição pretende fornecer informações de privacidade para os titulares dos dados pessoais.
- Quais são as salvaguardas para as transferências internacionais de dados.

O artigo 18 da LGPD é bem extenso e trata do direito que o titular tem de requisitar do controlador ações e informações específicas em relação ao tratamento realizado sobre os dados pessoais.

2.5.2.6 Identificar e avaliar os riscos

O art. 5º, XVII da LGPD preconiza que o Relatório de Impacto deve descrever **"medidas, salvaguardas e mecanismos de mitigação de risco"**.

Antes de definir tais medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular dos dados pessoais.

Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento.

Como exemplo, parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão a aplicação de medidas de segurança. Os parâmetros escalares adotados neste documento são apresentados na tabela a seguir:

Tabela 4 Parâmetros Escalares

CLASSIFICAÇÃO	VALOR
Baixo	5
Moderado	10
Alto	15

A figura a seguir apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco.

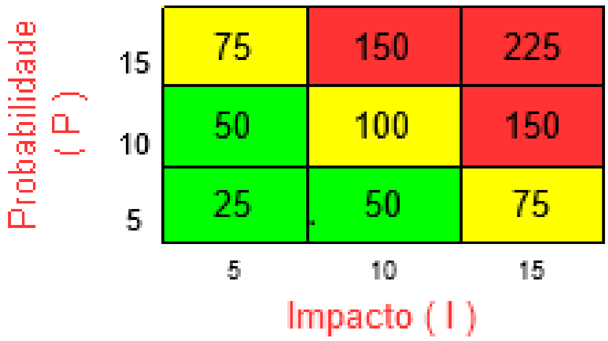


Figura 2 Matriz Probabilidade x Impacto

O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz apresentada pela **Figura 2**.

Risco enquadrado na região:

- verde, é entendido como baixo;
- amarelo, representa risco moderado; e
- vermelho, indica risco alto.

As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação e avaliação de riscos realizada no RIPD. Desse modo, é importante destacar que o gerenciamento de riscos relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos do órgão preconizada pela **Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016.**

Tendo em vista a seção 6 do modelo de **RIPD** constante do Anexo I, a identificação e avaliação de riscos envolve elencar os eventos de risco, a probabilidade, o impacto e o nível de risco.

A título de informação, é destacada a seguir uma tabela com lista não exaustiva de riscos de privacidade e de segurança da informação relacionados com a proteção de dados pessoais. O nível de probabilidade, impacto e nível de risco indicados são apenas exemplificativos, devendo ser avaliados de acordo com o contexto de cada instituição. Os treze primeiros itens representam riscos de privacidade obtidos da norma **ISO/IEC 29134:2017 seção 6.4.4**.

Lembrando que deve ser identificado qualquer risco que afete o tratamento de dados pessoais, independentemente de sua natureza (técnica, administrativa, de segurança da informação ou de privacidade).

Tabela 5 Risco referente ao tratamento de dados pessoais

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P[1]	I[2]	NÍVEL DE RISCO (P X I)[3]
R01	Acesso não autorizado.	10	15	**150**
R02	Modificação não autorizada.	10	15	**150**
R03	Perda	5	15	**75**
R04	Roubo	5	15	**75**
R05	Remoção não autorizada.	5	15	**75**
R06	Coleção excessiva.	10	10	**100**
R07	Informação insuficiente sobre a finalidade do tratamento.	10	15	**150**
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	**150**
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	**75**
R10	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais.	10	15	**150**
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	**50**
R12	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	**75**
R13	Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada, etc.).	5	15	**75**
R14	Reidentificação de dados pseudonimizados.	5	15	**75**

Legenda: P – Probabilidade; I – Impacto.

1. Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente; ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).
2. Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

3. Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

2.5.2.7 Identificar medidas para tratar os riscos

Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46).

Importante reforçar que as medidas para tratar os riscos podem ser: de segurança, técnicas ou administrativas.

A coluna "Medida(s)" pode ser preenchida com uma medida de segurança ou controle específico adotado para tratamento de cada risco identificado na etapa "Identificar e avaliar riscos".

A instituição nem sempre precisa eliminar todos os riscos. Nesse sentido, pode-se decidir que alguns riscos são aceitáveis - até um risco de nível alto –, devido aos benefícios do processamento dos dados pessoais e dificuldades de mitigação. **No entanto, se houver um risco residual de nível alto, é recomendável consultar a ANPD antes de prosseguir com as operações de tratamento dos dados pessoais.**

A seguir, são apresentados exemplos de medidas para lidar com os riscos a fim de demonstrar o preenchimento da tabela constante da seção 7 do **RIPD**, que consta no Anexo I.

Tabela 6 Exemplos de medidas para lidar com os riscos

RISCO	MEDIDA(S)	EFEITO SOBRE RISCO[1]	RISCO RESIDUAL[2]			MEDIDA(S) [3] APROVADA(S)
			P	I	(P X I)	
R01 Acesso não autorizado.	1. Controle de acesso Lógico.	Reduzir	5	10	**50**	Sim
	2. Desenvolvimento seguro.					
	3. Segurança em Redes.					

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6 do RIPD.

1. Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.
2. Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratá-lo.
3. Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

Neste momento, e a critério do responsável pela elaboração do RIPD, a coluna "Medida(s)" também pode ser preenchida de forma mais detalhada, indicando os principais aspectos da medida segurança ou controles de segurança adotados para tratar o risco. Esse procedimento propicia mais visibilidade em relação ao tratamento do risco.

2.5.2.8 Aprovar o Relatório

Esta etapa visa formalizar a aprovação do **RIPD** por meio da obtenção das assinaturas do responsável pela elaboração do **RIPD**, pelo encarregado e pelas autoridades que representam o controlador e operador.

O responsável pela elaboração do **Relatório** pode ser o próprio encarregado ou qualquer outra pessoa designada pelo controlador com conhecimento necessário para realizar tal tarefa.

2.5.2.9 Manter Revisão

O **RIPD** deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela instituição.

De uma forma geral, essa mudança pode ser motivada por alteração:

- significativa na finalidade do tratamento de dados pessoais;
- que impacte no processo de como esses dados são tratados;
- expressiva na quantidade de dados pessoais coletados; e
- no contexto do tratamento de dados resultantes de identificação de falha de segurança, uso de uma nova tecnologia, nova preocupação pública sobre o tipo de tratamento de dados realizado pela instituição ou vulnerabilidade de um grupo específico de titulares de dados pessoais.

Cumpre destacar que as orientações referentes à identificação da necessidade de elaborar ou atualizar o **RIPD** constantes do item 2.5.2.2 deste documento também contribuem para a identificação de casos em que o **Relatório de Impacto** deve ser atualizado.

A instituição deve manter revisão do **RIPD** a fim de demonstrar que avalia continuamente os riscos de tratamento de dados pessoais que surgem em consequência do dinamismo das transformações nos cenários tecnológico, normativo, político e institucional.

2.6TÉRMINO DO TRATAMENTO

Nos termos da LGPD, o término do tratamento de dados pessoais ocorre em quatro hipóteses:

(i) exaurimento da finalidade para os quais os dados foram coletados ou quando estes deixam de ser necessários ou pertinentes para o alcance desta finalidade;

(ii) fim do período de tratamento;

(iii) revogação do consentimento ou a pedido do titular, resguardado o interesse público;

(iv) determinação da autoridade nacional em face de violação do disposto na Lei.

Na incidência de qualquer uma das hipóteses acima, a Lei determina que os dados sejam eliminados, a não ser nos casos em que:

(i) remanesça o cumprimento de obrigação legal ou regulatória pelo controlador;

(ii) sejam necessários para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados;

(iii) ocorra a transferência a terceiro, desde que respeitados os requisitos de tratamento dispostos em Lei; e

(iv) seja utilizado exclusivamente pelo controlador, vedado seu acesso por terceiro, e desde que anonimizados.

No âmbito da Administração Pública, é importante que este dispositivo seja harmonizado com a legislação de arquivos, em especial com o que preceitua a Lei nº 8.159/1991, e suas regulamentações. Isso porque, desse ponto de vista, os dados pessoais coletados pelo poder público passam a constituir o que se denomina arquivo público (art. 7°) e a sua eliminação deverá obedecer, também, a classificação arquivística pertinente, de acordo com o valor arquivístico de cada documento. Além disso, a eliminação de documentos produzidos por instituições públicas e de caráter público é realizada mediante autorização da instituição arquivística pública, na sua específica esfera de competência (art. 9).

Assim, por exemplo, mesmo exaurida a finalidade precípua da coleta (primeira hipótese levantada), o dado pessoal poderá compor documento de valor permanente (quer por sua natureza histórica, probatória ou informativa) o qual tem natureza inalienável e imprescritível (art. 10).

3 O CICLO DE VIDA DO TRATAMENTO DOS DADOS PESSOAIS

O dado pessoal é coletado para atender a uma finalidade específica e pode, por exemplo, ser eliminado a pedido do titular dos dados[1] (LGPD, art. 18, IV), ao cumprimento de uma sanção aplicada pela Autoridade Nacional de Proteção de Dados (LGPD, art. 52, VI) ou ao término de seu tratamento (LGPD, art. 16). Dessa forma[1], percebemos a configuração de um ciclo que se inicia com a coleta e que determina a "vida" (existência) do dado pessoal durante um período de tempo, de acordo com certos critérios de eliminação.

É fundamental destacar que a LGPD considera como tratamento todas as operações realizadas com dados pessoais. Assim, a LGPD não adota qualquer tipo de segregação, considerando como tratamento, por exemplo, tanto a coleta quanto o armazenamento de dados pessoais, mesmo essas operações tratando de propósitos diferentes.

Para orientar a prática do tratamento e apresentar os ativos institucionais envolvidos, divide-se o ciclo de vida do tratamento dos dados pessoais em cinco fases: coleta, retenção, processamento, compartilhamento e eliminação.

Nesta seção, abordaremos o que é cada fase do ciclo de vida, a relação das fases do ciclo com as operações de tratamento da LGPD, os tipos de ativos organizacionais e o relacionamento desses ativos com as fases do ciclo de tratamento, destacando as ações a serem executadas em tais fases.

3.1 FASES DO CICLO DE VIDA

Para implementar o correto tratamento dos dados pessoais e as medidas correlatas, o órgão precisa conhecer os dados pessoais que gerencia e quais processos, projetos, serviços e ativos perpassam o **ciclo de vida do tratamento dos dados pessoais**.

O ciclo de vida do tratamento tem início com a coleta do dado e se encerra com a eliminação ou descarte. Cada fase do ciclo de vida tem correspondência com operações de tratamento definidas na LGPD. A fase coleta refere-se à coleta, produção, recepção de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, sistema de informação etc). A retenção corresponde ao arquivamento ou armazenamento de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, banco de dados, arquivo de aço etc). O processamento é qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação e extração e modificação de dados pessoais retidos pelo controlador. O compartilhamento, por sua vez, envolve qualquer operação de transmissão, distribuição, comunicação, transferência, difusão e uso compartilhamento de dados pessoais. Por fim, a eliminação é qualquer operação que visa excluir um dado ou conjunto de dados pessoais armazenados em banco de dados, bem como eliminação de documentos eletrônicos ou em papel em que constam dados pessoais. Esta fase também contempla o descarte dos ativos organizacionais (documentos, equipamentos, etc) nos casos necessários ao negócio da instituição.

A figura a seguir sintetiza as fases do ciclo de vida do tratamento de dados pessoais:

---

1 Ressalte-se que no caso de cumprimento de obrigação legal, como ocorre com a administração pública na maior parte dos casos, é autorizada a conservação do dado (LGPD, art. 16, I). Isso significa que, da mesma forma que o titular dos dados não precisa consentir o tratamento dos dados pessoais pela administração pública em casos determinados, também não é possível ao titular do dado solicitar a eliminação.



Figura 3 Ciclo de vida do tratamento dos dados pessoais

Coleta: obtenção, recepção ou produção de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, sistema de informação, etc.).

Retenção: arquivamento ou armazenamento de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, banco de dados, arquivo de aço, etc.).

Processamento: qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais.

Compartilhamento: qualquer operação que envolva transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais.

Eliminação: qualquer operação que visa apagar ou eliminar dados pessoais. Esta fase também contempla descarte dos ativos organizacionais nos casos necessários ao negócio da instituição.

A **Tabela 7** ilustra a relação entre as fases do ciclo de vida descrito nesta seção e as operações consideradas como tratamento pela LGPD.

Tabela 7 Relacionamento fases ciclo de vida X operações sobre dados pessoais.

DADOS PESSOAIS	
FASE DO CICLO DE TRATAMENTO	OPERAÇÕES DE TRATAMENTO - LGPD, ART. 5º, X
Coleta	Coleta, produção, recepção.
Retenção	Arquivamento e armazenamento.
Processamento	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação.
Compartilhamento	Transmissão, distribuição, comunicação, transferência e difusão.
Eliminação	Eliminação.

A operação de tratamento "acesso" (LGPD, art. 5º, X) está presente em todas as fases do ciclo de vida dos dados pessoais, pois de alguma forma temos que realizar acesso ao dado pessoal para viabilizar sua coleta, retenção, processamento, compartilhamento ou eliminação.

3.2 ATIVOS ORGANIZACIONAIS

É importante identificar quais ativos organizacionais estão envolvidos em cada fase do ciclo de vida do tratamento dos dados pessoais. Os **principais ativos** são: **bases de dados, documentos, equipamentos, locais físicos, pessoas, sistemas e unidades organizacionais**. A **Figura 4** apresenta os principais ativos envolvidos no ciclo de vida do tratamento dos dados.



Figura 4 Ativos envolvidos no ciclo de vida do tratamento dos dados.

A seguir, são apresentadas definições para os ativos envolvidos no ciclo de vida do tratamento dos dados pessoais.

Base de dados: é uma coleção de dados logicamente relacionados, com algum significado. Uma base de dados é projetada, construída e preenchida (instanciada) com dados para um propósito específico.

Documento: unidade de registro de informações, qualquer que seja o suporte e formato (Arquivo Nacional, 2005).

Equipamento: objeto ou conjunto de objetos necessário para o exercício de uma atividade ou de uma função.

Local físico: determinação do lugar no qual pode residir de forma definitiva ou temporária uma informação de identificação pessoal. Por exemplo, uma sala, um arquivo, um prédio, uma mesa, etc.

Pessoa: qualquer indivíduo que executa ou participa de alguma operação realizada com dados pessoais, como as que se referem a: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Sistema: qualquer aplicação, software ou solução de TI que esteja envolvida com as fases do ciclo de vida do tratamento dos dados pessoais: coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais.

Unidade organizacional: órgãos e entidades da Administração Pública.

3.3 RELACIONAMENTO DO CICLO VIDA DO TRATAMENTO DOS DADOS PESSOAIS COM ATIVOS ORGANIZACIONAIS

Para cada fase do ciclo de tratamento de dados é importante identificar os ativos organizacionais que estarão envolvidos.

Na fase de **Coleta** deve-se identificar os ativos envolvidos na coleta de dados pessoais. Esses dados podem entrar na organização por algum **documento físico**, algum **sistema** hospedado em algum **equipamento** localizado em **local físico** do órgão público. Podem ser coletados pela prestação de algum serviço externo ou serviço prestado pelo próprio órgão público por meio de alguma de suas **unidades organizacionais**.

Na fase de **Retenção**, deve-se avaliar os ativos utilizados para armazenar os dados pessoais. Esses dados podem estar armazenados em **bases de dados, documentos físicos, equipamentos ou sistemas**. É preciso considerar também as **unidades organizacionais** responsáveis pelo armazenamento e guarda dos dados, bem como os **locais físicos** onde estão localizados os ativos que armazenam esses dados. Se o armazenamento for em "nuvem", por exemplo, é necessário considerar o serviço de armazenamento contratado e/ou utilizado.

A fase de **Processamento** segue a mesma linha de raciocínio das anteriores. Identifica-se

os ativos onde são realizados os tratamentos dos dados. O tratamento pode ser realizado em **documento físico**, pode ser feito por um **sistema** interno ou contratado pelo órgão. É preciso identificar as **pessoas** (papeis organizacionais), **unidade organizacionais e equipamentos** envolvidos nesse tratamento. Onde estão **localizadas fisicamente** essas unidades organizacionais e os equipamentos envolvidos nesse tratamento também são importantes.

Na fase de **Compartilhamento** é preciso mapear os ativos envolvidos na distribuição ou divulgação dos dados pessoais para dentro e para fora do órgão público. Quais **sistemas** são usados para transmitir, exibir ou divulgar dados pessoais? Quais **pessoas** são destinatárias dessas informações? Quais **unidades organizacionais**, quais e**quipamentos** são usados para tal?

No que se refere à fase de **Eliminação**, deve-se avaliar os ativos que armazenam os dados pessoais que possam ser objeto de: solicitação de eliminação de dados a pedido do titular dos dados pessoais; ou descarte nos casos necessários ao negócio da instituição. Os dados pessoais a serem eliminados podem estar armazenados em ativos relacionados com **bases de dados, documentos físicos, equipamentos ou sistemas**, tais ativos também podem ser objeto de descarte. É necessário considerar também as **unidades organizacionais** responsáveis pelo armazenamento e guarda dos dados que possam ser objeto de eliminação ou descarte, bem como os **locais físicos** onde estão localizados os ativos que contenham dados a serem eliminados ou descartados. Se a eliminação do dado pessoal ou descarte do ativo tiver relação com solução em "nuvem", por exemplo, é preciso considerar o serviço de armazenamento contratado ou utilizado. Ainda, é preciso considerar as regras incidentes sobre os arquivos públicos.

Esse processo demanda esforço considerável, principalmente para grandes organizações. O ideal é que se estabeleçam ações de **mapeamento e análise dos processos organizacionais**, tendo em vista que, desta forma, o órgão conseguirá identificar de maneira mais eficaz os ativos descritos anteriormente.

Por exemplo, a **Figura 5** apresenta o relacionamento entre as fases do ciclo de tratamento de dados pessoais e os ativos que podem ser utilizados em cada etapa. É importante registrar, assim, que existem ativos presentes em todas as fases do ciclo (ex: Documento) e outros que estarão em apenas algumas delas (ex: Pessoa).

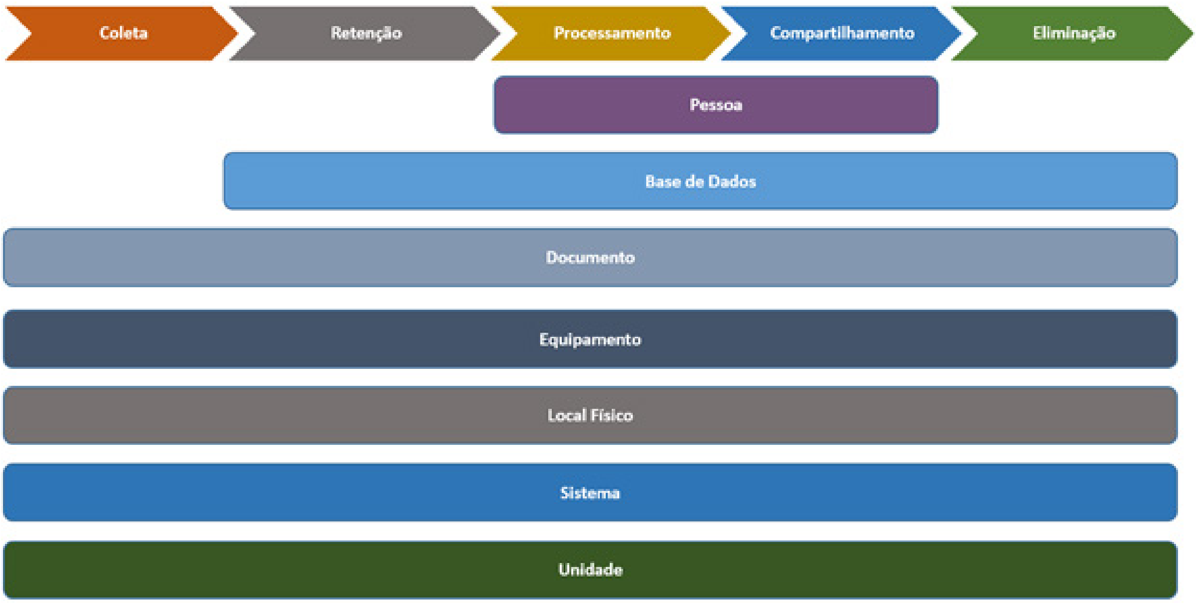


Figura 5 Ativos e fases do ciclo de vida dos dados pessoais.

Uma vez identificados os ativos, é necessário analisá-los para verificar quais medidas técnicas de segurança estão efetivamente implementadas nesses ativos, com vistas a prover a adequada proteção aos dados pessoais de que trata a LGPD. Recomenda-se a utilização de algum framework, boa prática ou norma técnica aplicável como a **ABNT NBR ISO/IEC 27001 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos; ABNT NBR ISO/IEC 27002 – Código de Prática para controles de segurança da informação; ABNT NBR ISO/IEC 27701 Técnicas de segurança — Extensão da ABNT NBR ISO/ IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos**

e diretrizes; ISO/IEC 29151 – Code of practice for personally identifiable information protection; CIS® (Center for Internet Security, Inc.®) Controls™ e ISO/IEC 29134 - Guidelines for privacy impact assessment. Além disso, é compulsória para toda a Administração Pública Federal brasileira a implementação das medidas de segurança dispostas pela **Instrução Normativa (IN) GSI/PR nº 1, de 13 de junho de 2008** e Normas Complementares decorrentes. A **IN GSI/PR nº 1/2018** disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta.

O resultado dessa análise vai determinar quais medidas de segurança devem ser implementadas em cada ativo e quais devem ser ajustadas para que o órgão público possua o adequado grau de proteção de dados exigido pela LGPD. A **Figura 6** apresenta esquema de mapeamento dos ativos e suas respectivas **medidas de segurança** implementadas (destacadas em verde) e não implementadas (destacadas em vermelho).

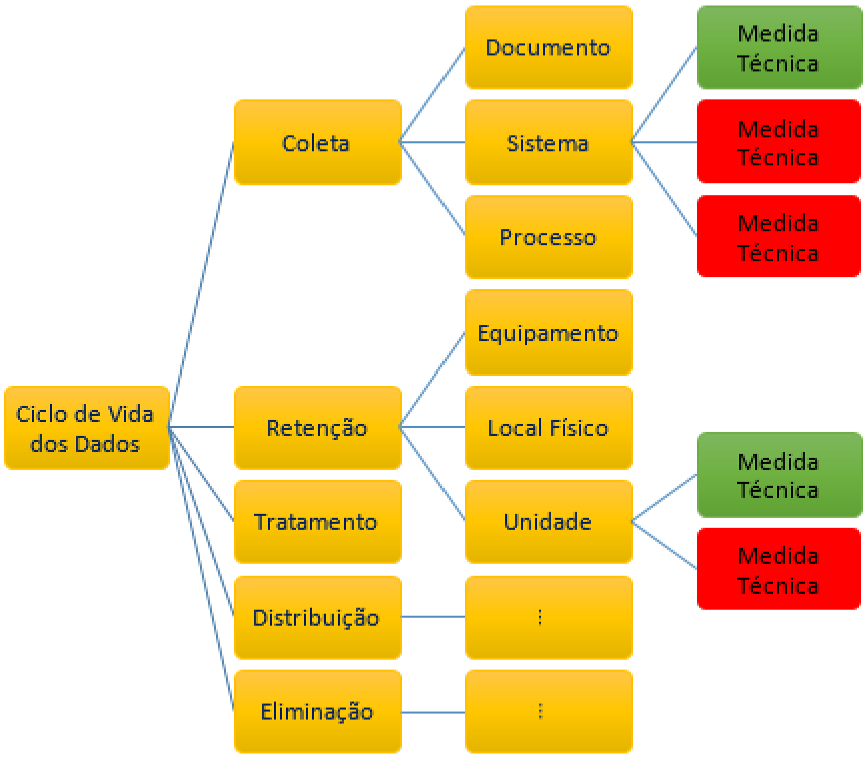


Figura 6 Ativos X fases do ciclo de tratamento X medidas de segurança

As medidas de segurança e os controles de segurança cibernética recomendados a aplicar nos ativos serão apresentados na seção 4.3 deste documento.

4 BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

4.1 PRIVACIDADE DESDE A CONCEPÇÃO E POR PADRÃO (PRIVACY BY DESIGN E BY DEFAULT)

4.1.1 Privacidade desde a concepção

Os agentes de tratamento ou qualquer outra pessoa que participe das fases do ciclo de vida do tratamento de dados pessoais são obrigados a assegurar a segurança da informação para proteção dos dados pessoais, pois ambas estão relacionadas.

Segundo o previsto pelo caput do art. 46 da LGPD, a proteção dos dados pessoais é alcançada por meio de **medidas de segurança**, técnicas e administrativas.

> **Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.**
>
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados: a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
>
> **§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.**

O art. 46, § 2º menciona que as **medidas de segurança**, técnicas e administrativas para proteção de dados pessoais deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. Isso apresenta um conceito fundamental para a proteção da privacidade dos dados pessoais denominado **Privacidade desde a Concepção** (do inglês Privacy by Design).

O conceito de Privacidade desde a Concepção significa que a privacidade e a proteção de dados devem ser consideradas desde a concepção e durante todo o ciclo de vida do projeto, sistema, serviço, produto ou processo. Tal privacidade pode ser alcançada por meio da aplicação dos 7 Princípios Fundamentais (Cavoukian, 2009) destacados nas próximas subseções deste tópico.

4.1.1.1 Proativo, e não reativo; preventivo, e não corretivo

A abordagem de Privacidade desde a Concepção (PdC) é caracterizada por medidas proativas e não reativas. Ou seja, essa abordagem antecipa e evita eventos invasivos de privacidade antes que eles aconteçam. Desse modo, não espera que riscos de privacidade se materializem nem ofereçam soluções para as infrações de privacidade após a ocorrência, mas visa impedir que eles ocorram. Em resumo, a Privacidade desde a Concepção vem antes do fato, não depois.

Se aplicada a tecnologias da informação, práticas organizacionais, projeto físico ou em rede de ecossistemas de informação, a PdC começa com um reconhecimento explícito do valor e dos benefícios de adoção de práticas de privacidade fortes, de forma precoce e consistente. Por exemplo, prevenindo a ocorrência de violações de dados, internas ou externas. Isso implica:

- um compromisso claro da alta administração em definir e fazer cumprir altos padrões de privacidade;

- um compromisso de privacidade comprovadamente compartilhado pelas comunidades de usuários e pelas partes interessadas e inserido em uma cultura de melhoria contínua; e
- métodos estabelecidos para reconhecer projetos de privacidade inadequados, antecipar práticas inadequadas de privacidade e corrigir quaisquer impactos negativos, muito antes de ocorrerem.

4.1.1.2 Privacidade deve ser o padrão dos sistemas de TI ou práticas de negócio

A privacidade por padrão procura oferecer o máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou prática de negócios. É uma forma de evitar que qualquer ação seja necessária por parte do titular dos dados pessoais para proteger a sua privacidade, pois ela já estará embutida no sistema, por padrão.

Esse princípio será melhor detalhado na seção 4.2.2 deste documento.

4.1.1.3 Privacidade incorporada ao projeto (design)

A privacidade deve estar incorporada ao projeto e arquitetura dos sistemas de TI e práticas de negócios. Isto significa que não deve ser considerada como complemento adicional, após o sistema, projeto ou serviço já estar em implementação ou em execução. O resultado é que a privacidade se torna um componente essencial da funcionalidade principal que está sendo entregue. A privacidade é parte integrante do sistema, sem diminuir a funcionalidade.

A privacidade deve ser incorporada às tecnologias, operações e arquiteturas de informação de maneira holística, integrativa e criativa:

- holística significa que contextos adicionais mais amplos devem sempre ser considerados;
- integrativa indica que todas as partes interessadas devem ser consultadas; e
- criativa, pois incorporar privacidade às vezes significa reinventar as escolhas atuais quando as alternativas forem inaceitáveis.

Para alcançar esse objetivo, deve-se adotar uma abordagem sistemática apoiada em padrões e frameworks reconhecidos, os quais devem dever ser revistos e passíveis de auditorias externas. Todas as práticas de informação equitativa precisam ser aplicadas com igual rigor a cada etapa do projeto e da operação.

O impacto do uso, configuração incorreta ou erros relativos à tecnologia, à operação ou à arquitetura de informações sobre a privacidade devem ser comprovadamente minimizados. Por isso, avaliações de impacto e risco na privacidade devem ser realizadas e publicadas, documentando claramente os riscos à privacidade e todas as medidas tomadas para mitigá-los. A seção 2.5 deste documento apresenta orientações referentes à elaboração de Relatório de Impacto à Proteção dos Dados Pessoais.

4.1.1.4 Funcionalidade total

A PdC não envolve simplesmente a formalização de declarações e compromissos de privacidade. Refere-se a satisfazer todos os objetivos do projeto, não apenas os objetivos de privacidade. A PdC é habilitadora duplamente em natureza, permitindo funcionalidade total com resultados reais e práticos.

Ao incorporar privacidade em uma determinada tecnologia, processo ou sistema, isso é realizado de uma forma que não comprometa a plena funcionalidade e permita que todas as exigências do projeto sejam atendidas.

A questão da privacidade é frequentemente vista como de nenhuma ou baixa relevância e que compete com a objetividade do projeto, com as capacidades técnicas de um produto ou serviço e com outros interesses das partes envolvidas. A PdC visa justamente contrapor essa visão, pois objetiva satisfazer todos os objetivos da instituição, e não somente os de privacidade. Evitando a pretensão de dicotomias falsas, como privacidade X segurança, o PdC demonstra que é possível — e mais desejável — ter ambos.

4.1.1.5 Segurança e proteção de ponta a ponta durante o ciclo de vida de tratamento dos dados

Por ser incorporado ao sistema antes de o primeiro elemento de informação ser coletado, a PdC estende-se por todo o ciclo de tratamento dos dados envolvidos no projeto, sistema ou serviço. Medidas fortes de segurança são essenciais para a privacidade, do início ao fim.

A privacidade deve ser protegida continuamente em todo o domínio e ao longo do ciclo de vida do tratamento dos dados em questão. Não deve haver lacunas na proteção ou na prestação de contas. O princípio "Segurança" tem relevância especial porque, em sua essência, sem segurança forte, não pode haver privacidade.

As instituições devem assumir a responsabilidade pela segurança dos dados pessoais, geralmente proporcional ao grau de sensibilidade, durante todo o ciclo de tratamento, consistente com os padrões que foram definidos por organismos reconhecidos de desenvolvimento de padrões.

Os padrões de segurança aplicados devem garantir a confidencialidade, integridade e disponibilidade dos dados pessoais durante todo o seu ciclo de tratamento, incluindo, entre outros, métodos de destruição segura, criptografia apropriada, e métodos fortes de controle de acesso e registro.

Na LGPD, a segurança é um princípio a ser observado no tratamento de dados pessoais, destacado pelo art. 6º, inciso VII.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> **VII - segurança:** utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

4.1.1.6 Visibilidade e Transparência

A PdC objetiva garantir a todos os interessados que, independentemente da prática ou tecnologia comercial envolvida, está de fato operando de acordo com as premissas e objetivos declarados, os quais devem ser objeto de verificação independente. Esse cenário pode ser sintetizado pelo seguinte lema: confie, mas verifique!

Visibilidade e transparência são essenciais para estabelecer responsabilidade e confiança. A avaliação independente deste princípio fundamental deve concentrar-se, especialmente, sobre os seguintes aspectos:

- **Responsabilização** - A coleta de dados pessoais implica um dever de cuidar de sua proteção. A responsabilidade por todas as políticas e procedimentos relacionados à privacidade deve ser documentada e comunicada conforme apropriado e atribuído a um indivíduo especificado. E ao transferir dados pessoais para terceiros, medidas equivalentes de proteção à privacidade devem ser asseguradas por contratos ou outros tipos de acordos formais.
- **Abertura** - Abertura e transparência são fundamentais para a prestação de contas. Informações sobre as políticas e práticas relacionadas ao gerenciamento de dados pessoais devem estar prontamente disponíveis para consulta dos titulares de dados. Mecanismos de reclamação e reparação dos dados pessoais devem ser estabelecidos e comunicados para os titulares dos dados.
- **Conformidade** - As etapas necessárias para monitorar, avaliar e verificar a conformidade com as políticas e procedimentos de privacidade devem ser estabelecidas.

A responsabilização, abertura e transparência estão expressas na LGPD pelos seguintes princípios destacados no art. 6º:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> **IV - livre acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e

a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; e

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

4.1.1.7 Respeito pela privacidade do usuário

Acima de tudo, a privacidade desde a concepção exige que as instituições respeitem os direitos dos titulares dos dados pessoais. Isso é alcançado por meio de medidas como padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que empoderem o titular dos dados.

Os melhores resultados da privacidade desde a concepção, geralmente, são aqueles projetados de acordo com os interesses e necessidades dos titulares dos dados pessoais, que têm o maior interesse em gerenciar seus próprios dados.

Empoderar os titulares de dados a desempenhar um papel ativo no gerenciamento de seus próprios dados pessoais pode ser o meio mais eficaz de verificação contra abusos de e uso indevido. O respeito à privacidade do titular dos dados pessoais é suportado pelos seguintes aspectos:

- **Consentimento ou hipótese de tratamento prevista em lei** - é necessário o consentimento livre e específico do titular dos dados para a coleta, uso ou divulgação de dados pessoais, exceto onde permitido por lei. As hipóteses de tratamento de dados pessoais e dados pessoais sensíveis estão preconizadas pelos arts. 7º e 11 da LGPD.
- **Precisão** - os dados pessoais devem ser precisos, completos e atualizados, conforme necessário para cumprir finalidades especificadas.
- **Acesso** - os titulares devem ter acesso aos seus dados pessoais e ser informados do uso e divulgação de tais dados. Os mencionados titulares devem ser capazes de contestar a precisão e integridade dos dados e alterá-los conforme apropriado.
- **Conformidade** - as instituições devem estabelecer mecanismos de reclamação e reparação e comunicar informações sobre eles ao público.

4.1.2 Privacidade desde a concepção

Os agentes de tratamento devem implementar medidas adequadas para garantir que, por padrão, apenas serão processados os dados pessoais necessários para cumprimento da(s) finalidade(s) específica(s) definida(s) pela instituição que desempenha o papel de controlador dos dados pessoais.

Essa obrigação de implementação significa que a instituição deve limitar a quantidade de dados pessoais coletados, extensão do tratamento, período de armazenamento e acessibilidade ao mínimo necessário para a concretização da finalidade do tratamento dos dados pessoais. Essa medida deve garantir, por exemplo, que nem todos os usuários dos agentes de tratamento tenham acesso ilimitado e por tempo indeterminado aos dados pessoais tratados pela instituição.

Na LGPD, a **Privacidade por Padrão** (do inglês Privacy by Default) está diretamente relacionada ao princípio da necessidade, expresso pelo art. 6º, inciso III.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

A privacidade por padrão é obtida por meio da adoção das seguintes práticas:

- **Especificação da finalidade** - os objetivos para os quais os dados pessoais são coletados, usados, retidos e divulgados devem ser comunicados ao titular dos dados antes ou no

momento em que as informações são coletadas. As finalidades especificadas devem ser claras, limitadas e relevantes em relação ao que se pretende ao tratar os dados pessoais.

- **Limitação da coleta** - a coleta de dados pessoais deve ser legal e limitada ao necessário para os fins especificados.
- **Minimização dos dados** - a coleta dos dados pessoais que possa identificar individualmente o titular de dados deve obter o mínimo necessário de informações pessoais. A concepção de programas, tecnologias e sistemas de informação e comunicação deve começar com interações e transações não identificáveis, como padrão. Qualquer vinculação de dados pessoais deve ser minimizada. A possibilidade de informações serem usadas para identificar o titular de dados deve ser minimizada.
- **Limitação de uso, retenção e divulgação** - o uso, retenção e divulgação de dados pessoais devem limitar-se às finalidades relevantes identificadas para o titular de dados, para as quais ele consentiu ou é exigido ou permitido por lei. Os dados pessoais serão retidos apenas pelo tempo necessário para cumprir as finalidades declaradas e depois eliminados com segurança.

Quando a necessidade ou uso de dados pessoais não forem claros, deve haver uma presunção de privacidade e o princípio da precaução deve ser aplicado. Dessa forma, as configurações padrão devem ser as de maior proteção à privacidade.

4.2 PADRÕES FRAMEWORKS E CONTROLES DE SEGURANÇA CIBERNÉTICA

É importante ter e seguir um conjunto de documentos para melhorar o gerenciamento de riscos de segurança cibernética. Um framework, por exemplo, apresenta condutas e recomendações para que sejam aplicados princípios e práticas recomendadas de gerenciamento de riscos para melhorar a segurança e a resiliência.

4.2.1 E-ping - Padrões de Interoperabilidade de Governo Eletrônico

A arquitetura ePING define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) na interoperabilidade de serviços de Governo Eletrônico, estabelecendo as condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral.

As áreas cobertas pela ePING estão segmentadas em:

- Interconexão;
- Segurança;
- Meios de Acesso;
- Organização e Intercâmbio de Informações;
- Áreas de Integração para Governo Eletrônico.

Mais informações: http://eping.governoeletronico.gov.br/

4.2.2 ABNT NBR ISO/IEC 27001:2013. Sistemas de gestão da segurança da informação

É uma norma do comitê técnico formado pela ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), aprovada e traduzida pela Associação Brasileira de Normas Técnicas (ABNT) - e transformada em uma Norma Brasileira (NBR) - de gestão de segurança da informação. São apresentados os requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de gestão da Segurança da Informação (SGSI), bem como os requisitos para avaliação e tratamento de riscos de segurança da informação, sempre com o foco nas necessidades da organização.

A ABNT NBR ISO/IEC 27001:2013 é dividida em 11 seções e Anexo A, sendo que as seções de 0 a 3 são introdutórias (não obrigatórias), e as seções de 4 a 10 são obrigatórias. Controles do Anexo A devem ser implementados apenas se declarados como apropriados e aplicáveis na Declaração de Aplicabilidade.

4.2.3 ABNT NBR ISO/IEC 27002: 2013. Código de Prática para controles de segurança da informação

Estipula melhores práticas para apoiar a implantação do SGSI, com diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização.

Esta norma contém 14 seções de controles de segurança da informação, de um total de 35 objetivos de controles e 114 controles. A parte principal da norma se encontra distribuída nas seguintes seções:

- Seção 5 – Política de Segurança da Informação;
- Seção 6 – Organização da Segurança da Informação;
- Seção 7 – Gestão de ativos;
- Seção 8 – Segurança em recursos humanos;
- Seção 9 – Segurança física e do ambiente;
- Seção 10 – Segurança das operações e comunicações;
- Seção 11 – Controle de acesso;
- Seção 12 – Aquisição, desenvolvimento e manutenção de sistemas;
- Seção 13 – Gestão de incidentes de segurança da informação;
- Seção 14 – Gestão da continuidade do negócio; e
- Seção 15 – Conformidade.

4.2.4 ABNT NBR ISO/IEC 27005:2019. Gestão de riscos de segurança da informação.

Esta norma apresenta diretrizes para o processo de gestão de riscos de segurança da informação de uma organização, atendendo particularmente aos requisitos de um SGSI, conforme a NBR ISO/IEC 27001.

As atividades do processo de gestão de riscos de segurança da informação, apresentadas na Seção 6, são detalhadas nas seguintes seções:

- Seção 7 - definição do contexto;
- Seção 8 - processo de avaliação de riscos;
- Seção 9 - tratamento do risco de segurança da informação;
- Seção 10 - aceitação do risco de segurança da informação;
- Seção 11 - comunicação e consulta do risco de segurança da informação; e
- Seção 12 - monitoramento e análise crítica de riscos de segurança da informação.

Os anexos apresentam Informações adicionais para as atividades de gestão de riscos de segurança da informação:

- Anexo A - Definindo o escopo e os limites do processo de gestão de riscos de segurança da informação;
- Anexo B - Identificação e valoração dos ativos e a avaliação do impacto são discutidas;
- Anexo C - Exemplos de ameaças comuns;
- Anexo D - Vulnerabilidades e métodos para avaliação de vulnerabilidades;

- Anexo E - Exemplos de abordagens para o processo de avaliação de riscos de segurança da informação;
- Anexo F - Restrições relativas à modificação do risco; e
- Anexo G - Diferenças nas definições entre a NBR ISO/IEC 27005:2011 e a NBR ISO/IEC 27005:2019.

4.2.5 ABNT NBR ISO/IEC 31000:2018. Gestão de riscos - Diretrizes.

É um documento com recomendações para gerenciar riscos enfrentados pelas organizações, podendo ser personalizado para qualquer contexto. A versão do ano de 2018 apresenta um guia mais claro e conciso, com o intuito de ajudar as organizações a usar os princípios de gerenciamento de risco para melhorar o planejamento e tomar melhores decisões.

4.2.6 ABNT NBR ISO/IEC 27701:2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.

Este documento especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) na forma de uma extensão das ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002. Visa a gestão da privacidade no contexto da organização.

4.2.7 Normativos do Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Os normativos do GSI/PR são de cumprimento obrigatório pelos órgãos e entidades da Administração Pública Federal, direta e indireta. Esses normativos são decorrentes de três instruções normativas, sendo a Instrução Normativa Nº 01 GSI/PR/2008 - Segurança da Informação e Comunicações regulamentada em 21 Normas Complementares, cuja implantação auxilia no aumento da maturidade da Segurança da Informação e elevação dos níveis de proteção dos dados.

As Normas Complementares decorrentes da Instrução Normativa Nº 01 GSI/PR/2008 podem ser encontradas no link http://dsic.planalto.gov.br/assuntos/editoria-c/normas-complementares/in-no-01-gsi-pr-2008-seguranca-da-informacao-e-comunicacoes

REFERÊNCIAS BIBLIOGRÁFICAS

- Arquivo Nacional. Dicionário Brasileiro de Terminologia Arquivística. 2005. Disponível em: <http://www.arquivonacional.gov.br/images/pdf/Dicion_Term_Arquiv.pdf>. Acesso em: 20 ago. 2019.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2013. Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação.
- ______. ABNT NBR ISO/IEC 27001:2013. Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.
- ______. ABNT NBR ISO/IEC 27005:2011. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.
- ______. ABNT NBR ISO/IEC 27701:2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes.
- ______. ABNT NBR ISO/IEC 29134:2017. Information technology – Security techniques – Guidelines for privacy impact assessment.
- ______. ABNT NBR ISO/IEC 29151:2017. Information technology – Security techniques – Code of practice for personally identifiable information protection.
- ______. ABNT NBR ISO/IEC 31000:2018. Gestão de riscos - Diretrizes.
- BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa nº 01, de 13 de junho de 2008. Brasília, DF, GSI/PR, 2008. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/52>. Último acesso em: 08 abr. 2019.
- BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Portaria Nº 93, de 26 de setembro de 2019. Brasília, DF, GSI/PR, 2019. Aprova o Glossário de Segurança da Informação. Disponível em: < http://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663>. Último acesso em: 19 fev. 2020.
- BRASIL. Presidência da República. Casa Civil. Decreto Nº 9.637, de 26 de dezembro de 2018. Institui a Política de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm>. Acesso em: 08 abr. 2019.
- BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm#art1>. Acesso em: 09 abr. 2019.
- BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o

uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 09 abr. 2019.

- BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 09 abr. 2019.
- BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Constituição da República Federativa do Brasil. Brasília, DF, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 09 abr. 2019.
- BRASIL. Ministério do Planejamento Desenvolvimento e Gestão. Guia de Gestão de Processos do Governo, 2011. Disponível em: <http://www.gespublica.gov.br/content/guia-de-gest%C3%A3o-de-processos>. Acesso em: 20 ago. 2019.
- BRASIL. Presidência da República. Casa Civil. Decreto Nº 8.936, de 19 de dezembro de 2016. Institui a Plataforma de Cidadania Digital e dispõe sobre a oferta dos serviços públicos digitais, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/Decreto/D8936.htm>. Acesso em: 20 ago. 2019.
- Cavoukian, Ann. Privacy by Design: The 7 Foundational Principles. August, 2009. Disponível em: <https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%207%20Foundational%20Principles.pdf>. Acesso em: 13 jan. 2020.
- CENTER for Internet Security. The 20 CIS Controls & Resources. April, 2019. Disponível em: < https://www.cisecurity.org/controls/cis-controls-list/ >. Acesso em: 20 out. 2019.
- PROJECT MANAGEMENT INSTITUTE. Um Guia de Conhecimento em Gerenciamento de Projetos. Guia PMBOK 5ª edição. Project Management Institute, 2013.

ANEXO I

RELATÓRIO DE IMPACTO

À PROTEÇÃO DE DADOS PESSOAIS

<Local>, <dia> de <mês> de <ano>

Histórico de Revisões

DATA	VERSÃO	DESCRIÇÃO	AUTOR
xx/xx/20xx	1.0	Conclusão da primeira versão do relatório	xxxx
xx/xx/20xx	2.0	Revisão do relatório após análise do controlador, operador e encarregado.	xxxx

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

OBJETIVO
O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. **Referência:** Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1. IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador

Operador

Encarregado

E-mail Encarregado	Telefone Encarregado

2. NECESSIDADE DE ELABORAR O RELATÓRIO

3. DESCRIÇÃO DO TRATAMENTO

3.1 NATUREZA DO TRATAMENTO

3.2 ESCOPO DO TRATAMENTO

3.3 CONTEXTO DO TRATAMENTO

3.4 FINALIDADE DO TRATAMENTO

4. PARTES INTERESSADAS CONSULTADAS

5. NECESSIDADE E PROPORCIONALIDADE

6. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P[1]	I[2]	NÍVEL DE RISCO (P X I)[3]

Legenda: P – Probabilidade; I – Impacto.

1. Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente; ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).
2. Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).
3. Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

7. MEDIDAS PARA TRATAR OS RISCOS

RISCO	MEDIDA(S)	EFEITO SOBRE RISCO[1]	RISCO RESIDUAL[2]			MEDIDA(S)[3] APROVADA(S)
			P	I	(P X I)	

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6 do RIPD.

1. Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.
2. Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratá-lo.
3. Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

8. APROVAÇÃO

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADO
____________________ <Nome do responsável> **Matrícula/SIAPE:** xxxxx <Local>, <dia> de <mês> de <ano>	____________________ <Nome do responsável> **Matrícula/SIAPE:** xxxxx <Local>, <dia> de <mês> de <ano>
AUTORIDADE REPRESENTANTE DO CONTROLADOR	**AUTORIDADE REPRESENTANTE DO OPERADOR**
____________________ <Nome do responsável> **Matrícula/SIAPE:** xxxxx <Local>, <dia> de <mês> de <ano>	____________________ <Nome do responsável> **Matrícula/SIAPE:** xxxxx <Local>, <dia> de <mês> de <ano>

ANEXO II

PREVISÕES NORMATIVAS QUE AUTORIZAM TRATAMENTO DE DADOS

Lei n° 9.507/1997, que regula o direito de acesso a informações e disciplina o rito processual do habeas data.

Data do ato	12/11/1997
Data da publicação no DOU	13/11/1997
Vigência (vacatio legis)	Art. 22. Esta Lei entra em vigor na data de sua publicação.
Acesso	http://www.planalto.gov.br/ccivil_03/LEIS/L9507.htm

Lei n° 9.784/1999, que regula o processo administrativo no âmbito da Administração Pública Federal.

Data do ato	29/01/1999
Data da publicação no DOU	01/02/1999 e retificado em 11/03/1999
Vigência (vacatio legis)	Art. 70. Esta Lei entra em vigor na data de sua publicação.
Acesso	http://www.planalto.gov.br/ccivil_03/LEIS/L9784.htm

Lei n° 12.527/2011 (Lei de Acesso à Informação), que regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

Data do ato	18/11/2011
Data da publicação no DOU	18/11/2011
Vigência (vacatio legis)	Art. 47. Esta Lei entra em vigor 180 (cento e oitenta) dias após a data de sua publicação.
Acesso	http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm

Decreto n° 7.724/2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.

Data do ato	16/05/2012
Data da publicação no DOU	16/05/2012 e 18/05/2012
Vigência (vacatio legis)	Art. 76. Este Decreto entra em vigor em 16 de maio de 2012.
Acesso	http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Decreto/D7724.htm

Lei n° 12.965/2014 (Marco Civil da Internet), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Data da Lei	23/04/2014
Data da publicação no DOU	24/04/2014
Vigência (vacatio legis)	Art. 32. Esta Lei entra em vigor após decorridos 60 (sessenta) dias de sua publicação oficial.
Acesso	http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm#art32

Decreto n° 8.771/2016, que regulamenta a Lei nº 12.965, de 23 de abril de 2014, (Marco Civil da Internet), para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

Data do ato	11/05/2016
Data da publicação no DOU	11/05/2016
Vigência (vacatio legis)	Art. 22. Este Decreto entra em vigor trinta dias após a data de sua publicação.
Acesso	http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm

Decreto nº 8.936/2016, que institui a Plataforma de Cidadania Digital e dispõe sobre a oferta dos serviços públicos digitais, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.

Data do ato	19/12/2016
Data da publicação no DOU	20/12/2016
Vigência (vacatio legis)	Art. 10. Este Decreto entra em vigor na data de sua publicação.
Acesso	http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8936.htm

Lei nº 13.444/2017, que dispõe sobre a Identificação Civil Nacional (ICN).

Data do ato	11/07/2017
Data da publicação no DOU	12/05/2017
Vigência (vacatio legis)	Art. 13. Esta Lei entra em vigor na data de sua publicação.
Acesso	http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13444.htm

Lei nº 13.460/2017, que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.

Data do ato	26/06/2017
Data da publicação no DOU	27/06/2017
Vigência (vacatio legis)	Art. 25. Esta Lei entra em vigor, a contar da sua publicação, em: I - trezentos e sessenta dias para a União, os Estados, o Distrito Federal e os Municípios com mais de quinhentos mil habitantes; II - quinhentos e quarenta dias para os Municípios entre cem mil e quinhentos mil habitantes; e III - setecentos e vinte dias para os Municípios com menos de cem mil habitantes.
Acesso	http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Lei/L13460.htm

Decreto n° 9.278/2018, que regulamenta a Lei nº 7.116, de 29 de agosto de 1983, que assegura validade nacional às Carteiras de Identidade e regula sua expedição.

Data do ato	05/02/2018
Data da publicação no DOU	06/02/2018
Vigência (vacatio legis)	Art. 24. Este Decreto entra em vigor na data de sua publicação.
Acesso	http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9278.htm

Lei n° 13.709/2018, Lei Geral de Proteção dos Dados – LGPD.

Data do ato	14/08/2018
Data da publicação no DOU	15/08/2018
Vigência (vacatio legis)	Art. 65. Esta Lei entra em vigor: (Redação dada pela Lei nº 13.853, de 2019) I - dia 28 de dezembro de 2018, quanto aos arts. 55-A, 55-B, 55-C, 55-D, 55-E, 55-F, 55-G, 55-H, 55-I, 55-J, 55-K, 55-L, 58-A e 58-B; e (Incluído pela Lei nº 13.853, de 2019) II - 24 (vinte e quatro) meses após a data de sua publicação, quanto aos demais artigos. (Incluído pela Lei nº 13.853, de 2019)
Acesso	http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Decreto n° 9.492/2018, que regulamenta a Lei nº 13.460, de 26 de junho de 2017 , que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública federal, institui o Sistema de Ouvidoria do Poder Executivo federal, e altera o Decreto nº 8.910, de 22 de novembro de 2016, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Transparência, Fiscalização e Controladoria-Geral da União.

Data do ato	05/09/2018
Data da publicação no DOU	06/09/2018
Vigência (vacatio legis)	Art. 28. Este Decreto entra em vigor na data de sua publicação.
Acesso	http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Decreto/D9492.htm

Decreto n° 9.723/2019, que altera o Decreto nº 9.094, de 17 de julho de 2017, o Decreto nº 8.936, de 19 de dezembro de 2016, e o Decreto nº 9.492, de 5 setembro de 2018, para instituir o Cadastro de Pessoas Físicas - CPF como instrumento suficiente e substitutivo da apresentação de outros documentos do cidadão no exercício de obrigações e direitos ou na obtenção de benefícios e regulamentar dispositivos da Lei nº 13.460, de 26 de junho de 2017.

Data do ato	11/03/2019
Data da publicação no DOU	12/03/2019 e 18/03/2019
Vigência (vacatio legis)	Art. 7º Este Decreto entra em vigor na data de sua publicação.
Acesso	http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9723.htm

Lei n° 13.853/2019, que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

Data do ato	08/07/2019
Data da publicação no DOU	09/07/2019
Vigência (vacatio legis)	Art. 4º Esta Lei entra em vigor na data de sua publicação
Acesso	http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2

Decreto n° 10.046/2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.

Data do ato	09/10/2019
Data da publicação no DOU	10/10/2019
Vigência (vacatio legis)	Art. 35. Este Decreto entra em vigor na data de sua publicação.
Acesso	http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm

Derrubada de vetos da **Lei n° 13.853/2019** pelo Congresso Nacional.

Data do ato	19/12/2019
Data da publicação no DOU	20/12/2019
Vigência (vacatio legis)	Art. 4º Esta Lei entra em vigor na data de sua publicação
Acesso	http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2